NORTEL

Nortel Switched Firewall 5100 Series Release 2.3.3

Browser-Based Interface User’s Guide

part number: 216383-D, October 2005

4655 Great America Parkway
Santa Clara, CA 95054
Phone 1-800-4Nortel
http://www.nortel.com

Contents

Preface

This *Quick Guide* describes the Nortel Switched Firewall Browser-Based Interface (BBI). The components and features of the BBI can be used as an alternative to the Nortel Switched Firewall Command Line Interface (CLI) documented in the *Nortel Switched Firewall 2.3.3 User's Guide and Command Reference,* (213455-L).

Who should use this book

This *Quick Guide* is intended for network installers and system administrators engaged in configuring and maintaining a network. Installers and administrators must be familiar with Ethernet concepts and IP addressing.

How this book is organized

The chapters in this book are organized as follows:

Chapter 1, Introduction,on page 11 describes how to enable and access the BBI.

Chapter 2, Basics of the Browser-Based Interface, on page 17 describes the BBI global commands, the BBI page components, and how to access the context-sensitive online Help for referencing page fields, buttons, and labels.

Chapter 3, Browser-Based Interface forms reference, on page 33 describes in detail all of the forms associated with the BBI.

Typographic conventions

The following table describes the typographic styles used in this book.

Table 1 Typographic conventions

Typeface or Symbol	Meaning	Example
`AaBbCc123`	This fixed-width type is used for names of commands, files, and directories used within the text.	**View the** `readme.txt` **file.**
	It also depicts on-screen computer output and prompts.	`Main#`
AaBbCc123	This italicized type shows book titles, special terms, or words to be emphasized.	**Read your *User's Guide* thoroughly.**
AaBbCc123	This fixed-width, bold type appears in command examples. It shows text that must be typed in exactly as shown.	`Main#` **sys**
<*AaBbCc123*>	Italicized type within angle brackets appears in command examples as a parameter placeholder. Replace the indicated text with the appropriate real name or value when using the command. Do not type the brackets.	**To establish a Telnet session, enter:** `host#` **telnet** <*IP address*>
[ ]	Command items shown inside square brackets are optional and can be used or excluded as the situation demands. Do not type the brackets.	`host#` **ls [-a]**
|	Command items separated by the vertical bar depict a list of possible values, only one of which should be entered. The vertical bar is considered to mean "or."	`System#` **autoneg on|off**
	This can also be used to separate different selections within a window-based menu bar.	**Select Edit | Copy from the window's menu bar.**
`<Key>`	Non-alphanumeric keyboard items are shown in regular type inside brackets. When directed, press the appropriate key.	**Press the <Enter> key.**

How to get help

This section explains how to get help for Nortel products and services.

Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site at: www.nortel.com/support.

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products.

Use the Nortel Technical Support web site to do the following:

- download technical information, including the following items:
  - software
  - documentation
  - product bulletins
- search the Technical Support web site and the Nortel Knowledge Base for answers to technical questions
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the telephone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support web site, you can get help over the telephone from a Nortel Solutions Center. You must have a Nortel support contract to use the Nortel Solutions Center.

To reach a Nortel Solutions Center, do one of the following;

- In North America, call 1–800–4NORTEL (1–800–466–7835).
- Outside North America, go to the following web site to obtain the telephone number for your region: www.nortel.com/callus.

Using an Express Routing Code to get help from a specialist

You can find Express Routing Codes (ERC) for many Nortel products and services on the Nortel Technical Support web site. ERCs allow you to connect directly to service and support organizations based on specific products or services.

To locate the ERC for your product or service, go to www.nortel.com/erc.

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

CHAPTER 1
Introduction

This chapter explains how to enable the Browser-Based Interface (BBI), set up your web browser, and launch the BBI to access the Nortel Switched Firewall (NSF) system-management features from your web browser.

Characteristics of the BBI

Following are the characteristics of the BBI:

- Intuitive interface structure.
- Configuration and monitoring functions similar to those available through the Command Line Interface (CLI).
- Access using HTTP, or secure HTTPS using Secure Socket Layer (SSL).
- No installation required; the BBI is part of the Firewall OS software.
- Upgrades with future software releases (as available).
- Runs up to ten BBI sessions simultaneously.
- Online context-sensitive Help for each BBI page.
- Online task-based Help for a variety of common procedures from each BBI page.

Getting started

Requirements

Following are the requirements to enable the BBI:

- An installed Nortel Switched Firewall
- A Check Point policy to allow management station access for HTTP or HTTPS traffic
- A PC or workstation with network access to the Firewall host IP address
- A Frame-capable web browser software, such as the following:
  - Netscape Navigator 4.6 or higher
  - Internet Explorer 5.5 or higher
- JavaScript enabled in your web browser
- Java 2 Runtime Environment SE plug-in, version 1.2.4-01 or higher

NOTE – JavaScript is different from Java. Ensure that JavaScript is enabled in your web browser.

Enabling the BBI

Before you can access the BBI, you must perform some configuration at the CLI. For information about accessing and using the CLI, see the *Nortel Switched Firewall 2.3.3 User's Guide and Command Reference,*(213455-L).

CLI configuration tasks

Following are the CLI configuration tasks required to enable access to the BBI:

- Enable the BBI.
- Generate a temporary certificate (if using HTTPS).
- Apply the changes.
- Use the access list to permit remote access to trusted clients.
- Use the Check Point SmartDashboard on your SMART Client to add a security policy that allows BBI traffic.

Enabling the BBI

You can enable the BBI for HTTP, HTTP and HTTPS, or you can fully disable the BBI. **TIP**: The default setting for the BBI is enabled for HTTP access and disabled for HTTPS access.

NOTE – HTTP is not a secure protocol. All data (including passwords) between an HTTP client and the Nortel Switched Firewall is not encrypted and is subject only to weak authentication. If secure remote access is required, use HTTPS.

To explicitly allow remote BBI access, enter the following commands in the CLI:

- To enable HTTP access:

```
>> # /cfg/sys/adm/web/http/ena
```

- To enable HTTPS access using SSL:

```
>> # /cfg/sys/adm/web/ssl/ena
```

Generating a temporary certificate if using HTTPS

An SSL server certificate is required for HTTPS access to the BBI. The Firewall can generate a temporary, self-signed certificate. Use the following commands to create a default certificate:

```
>> SSL configuration# certs/serv/gen <Name> <Country code> <Key size>
Do you want to generate a self-signed certificate with the generated
Key? y
```

where *Name* is the common name that appears on the certificate, *Country code* is a two-letter code (US for the United States of America, CA for Canada, JP for Japan, and so on), and *Key size* is 512, 1024, or 2048 bits. For example:

```
>> SSL configuration# certs/serv/gen Nortel US 1024
```

NOTE – When you log in to the BBI with the temporary certificate, you are warned that the certificate is not signed or authenticated. Permit use of the temporary certificate only during initial configuration, where the system is not attached to active networks that can be a source of attack. Install a signed and authenticated certificate prior to connecting any untrusted network.

Applying the changes.

```
>> SSL configuration# apply
```

Using the access list to permit remote access to trusted clients

If you already configured the access list for Telnet or SSH, you need not repeat the process. Otherwise, to permit access to only trusted clients, see the *Nortel Switched Firewall 2.3.3 User's Guide and Command Reference,* Part No. 213455-L.

Adding a security policy that allows BBI traffic

Use the Check Point SmartDashboard on your SMART Client to add a security policy that allows BBI traffic.

The firewall policy should be constructed as follows:

- Source: IP address of the SMART Client or IP address range of the management network
- Destination: Host IP address of the Firewall
- Service: HTTP for non-secure access, or SSL for HTTPS access
- Action: Allow—select **Nortel Switched Firewall**

Setting up the web browser

Most web browsers work with JavaScript by default and require no additional setup. Check the features and configuration of your web browser to ensure JavaScript is enabled.

NOTE – JavaScript is not the same as Java. Ensure that JavaScript is enabled in your web browser.

Starting the BBI

When the Firewall and browser setup is complete, use the following steps to launch the BBI:

1. Start your web browser.
2. Enter one of the following in the URL field of the web browser:
   a) host IP address
   b) host IP address as a name (when IP address is assigned a name on the local domain name server)

c) MIP address

d) virtual IP address (see Using the VRRP virtual IP address to access the NSF BBI)

The NSF login window opens.

3. Log in (see Logging in).

4. Allow the main page to load (see Loading the main page on page 16).

Using the VRRP virtual IP address to access the NSF BBI

To use the VRRP virtual IP address for firewall access by web browser, enable management support for the VRRP interface.

Use the following CLI command to enable management support for the VRRP interface:

```
/cfg/net/if #/mgmt/ena/apply
```

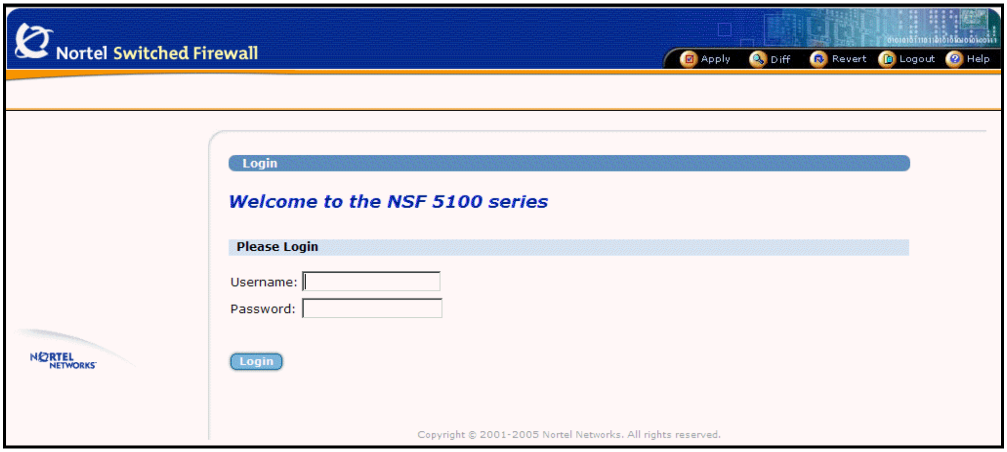
The virtual IP address is specified with the ip1 or ip2 command in the CLI menu. For more information, see the *Nortel Switched Firewall 2.3.3 User's Guide and Command Reference,* Part No. 213455-L.

Using the VRRP interface IP address enhances firewall security, because users can configure the VRRP interface with the user-defined CheckPoint policies. SSI traffic is separate from the CheckPoint policies.

Logging in

To log in, enter the account name and password for the system administrator or operator account (see Figure 1 on page 16). For more login and password information, see the *Nortel Switched Firewall 2.3.3 User's Guide and Command Reference,* (213455-L).

Figure 1 NSF Login window



Login

Welcome to the NSF 5100 series

Please Login

Username:

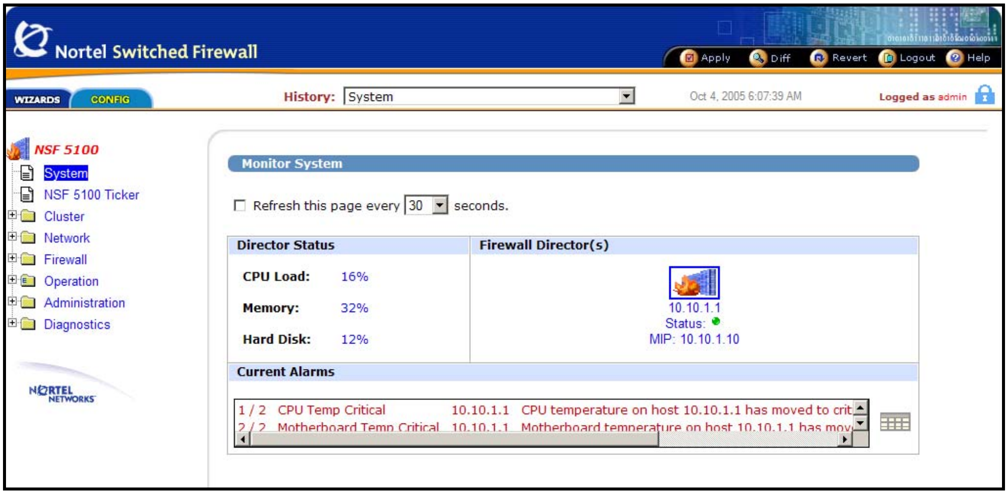
Password:

Copyright © 2001-2005 Nortel Networks. All rights reserved.

Loading the main page

When the valid account name and password combination is entered on the login window, the BBI default page appears in your browser viewing window (see Figure 2).

Figure 2 NSF BBI main page



History: System

Oct 4, 2005 6:07:39 AM

Logged as admin

Monitor System

□ Refresh this page every 30 seconds.

Director Status	Firewall Director(s)
CPU Load: 16%	10.10.1.1 Status: ● MIP: 10.10.1.10
Memory: 32%	
Hard Disk: 12%	

Current Alarms

1 / 2	CPU Temp Critical	10.10.1.1	CPU temperature on host 10.10.1.1 has moved to crit
2 / 2	Motherboard Temp Critical	10.10.1.1	Motherboard temperature on host 10.10.1.1 has mov

NOTE – A delay of a few seconds can occur while the default page collects data from all of the cluster components. Do not stop the browser while loading is in progress.

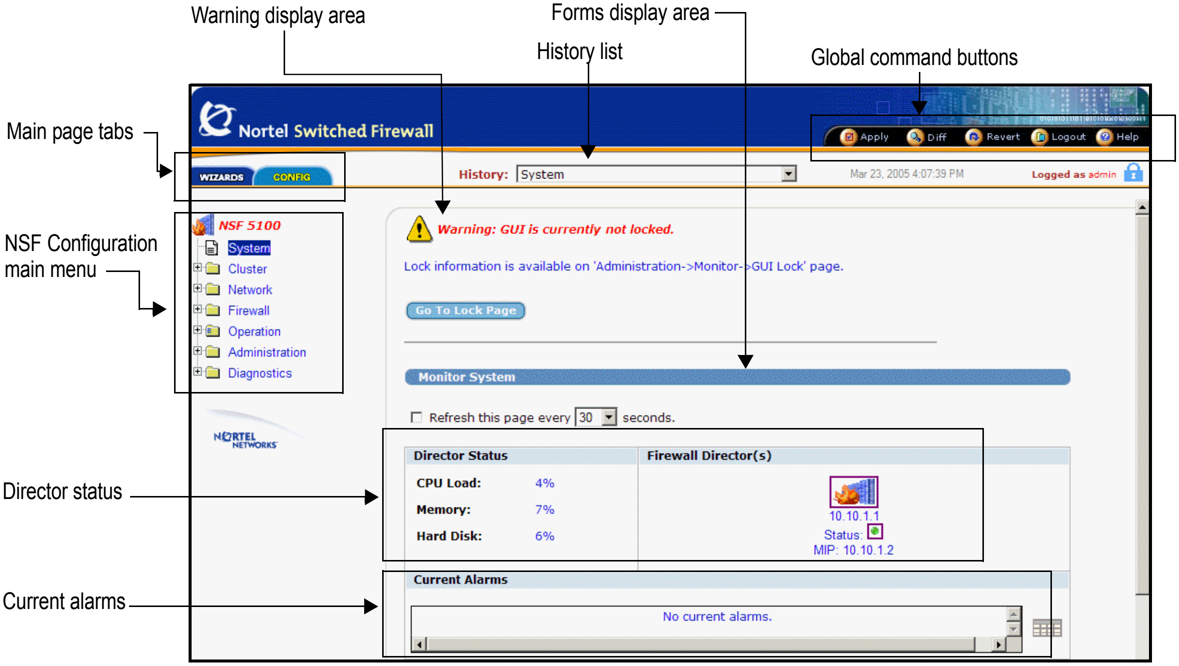
CHAPTER 2

Basics of the Browser-Based Interface

Interface components

The Nortel Switched Firewall (NSF) Browser-Based Interface (BBI) main page has eight component areas (see Figure 3).

Figure 3 NSF BBI main page



History: System

Mar 23, 2005 4:07:39 PM

Logged as admin

Warning: GUI is currently not locked.

Lock information is available on 'Administration->Monitor->GUI Lock' page.

☐ Refresh this page every 30 seconds.

Director Status		Firewall Director(s)
CPU Load:	4%	10.10.1.1 Status: MIP: 10.10.1.2
Memory:	7%	
Hard Disk:	6%	

Current Alarms

No current alarms.

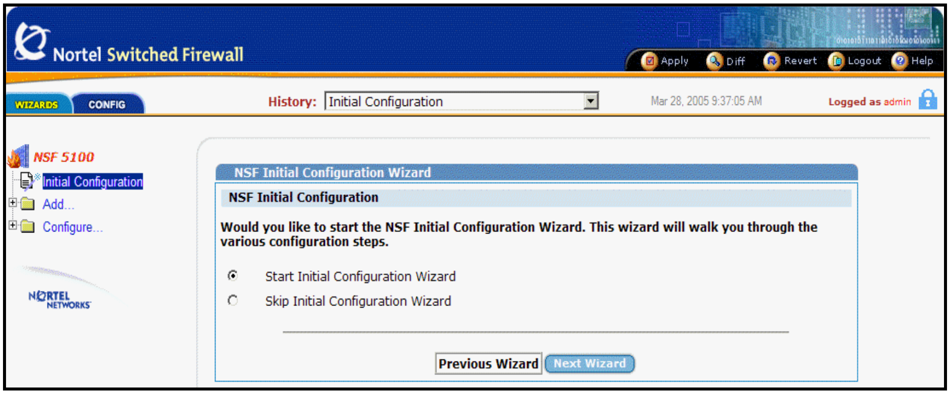
- Main page tabs

  The two main page tabs are Wizards and Config (see Figure 3 on page 17).

  - □ Wizards provides access to wizards that guide users through the processes of initial configuration, interface and bridge addition, Check Point Firewall configuration, routes and gateway configuration, DHCP Relay configuration, and OSPF configuration (see Figure 4 and Figure 5). To use the wizards, select **Initial Configuration**, **Add**, or **Configure**, and follow the instructions on the page. Click the plus sign (+) adjacent to a selection to expand it and reveal its associated subcategories. To see each of the initial Wizards pages, see Chapter 3, Browser-Based Interface forms reference.

  - □ Config is the default tab for the BBI main page and provides access to all of the monitoring and configuration functions (see Figure 6 on page 20).

Figure 4 NSF Wizards main page



History: Initial Configuration

Mar 28, 2005 9:37:05 AM

Logged as admin

NSF Initial Configuration Wizard

NSF Initial Configuration

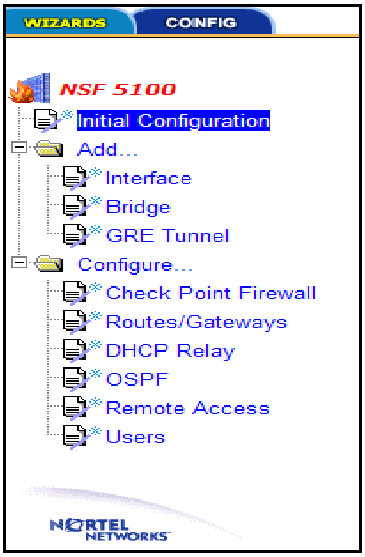
Would you like to start the NSF Initial Configuration Wizard. This wizard will walk you through the various configuration steps.

● Start Initial Configuration Wizard

○ Skip Initial Configuration Wizard

Wizards menu shows the selections available on the Wizards menu tree.

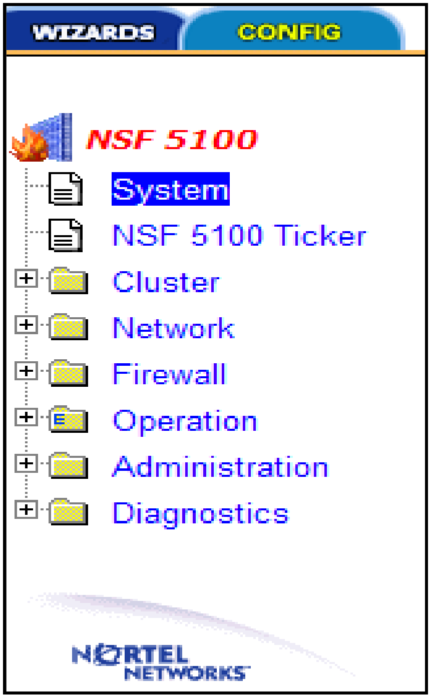
Figure 5 Wizards menu



- NSF Config main menu tree

  Each of the selections on the Config main menu tree represents a page, called a form, which provides a method to monitor or configure the NSF (see Figure 3 on page 17 and Figure 6).

  Figure 6 NSF Config main menu

  Each main menu category offers subcategories, providing a further level of control or detailed information. Click the plus sign (+) adjacent to a selection to expand it and reveal its associated subcategories.

  For detailed information about the forms, see Chapter 3, Browser-Based Interface forms reference, on page 33.

- Warning display area

  The Warning display area provides important warnings for the user, such as information about CLI users logged in or the status of the GUI lock. Any user logged in as administrator (username *admin*) can activate the GUI lock before changing or creating a configuration. See Figure 75 on page 107.

- History list

  The History list displays the path to the current page. Up to nine of the most recently visited pages are listed, most recent first. **TIP**: Click a list item to go directly to that page.

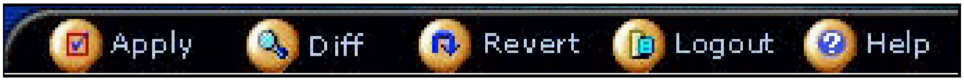
- Forms display area

  The Forms display area contains fields that display information or allow you to specify information for configuring the system. The fields are different for each subpage.

- Global command buttons

  The global command buttons are always available at the top of each form (see Figure 3 on page 17 and Figure 7).

  Figure 7 Global command buttons

  The global commands summon forms used for saving, examining, or canceling configuration changes, for logging out, and for displaying Help information for the current page (see Global command forms on page 24).

- Director status appears on the left side of the forms display area, under the Monitor System bar. Director status summarizes the status of the cluster, including CPU, memory, and hard disk. The Firewall icon appears on the right side of the forms display area under the Monitor System bar. **TIP**: Click the Firewall icon to go directly to the Administration/Monitor/Director(s) form (see Figure 71 on page 103).

  - The Firewall host IP address and Management IP address (MIP) appear under the Firewall icon.

  - The status icon for the firewall appears between the addresses.

    TIP: Click the Firewall icon to go directly to the Administration/Monitor/Director(s) form (see Figure 71 on page 103).

    - When the status icon is green, the firewall is operating, and when the status icon is red, the firewall is offline.

- Current alarms provides the current status of all active alarms.

Basic operation

The Browser-Based Interface for the Nortel Switched Firewall provides a variety of levels of control. **TIP**: To access the full functionality of the BBI, you must log in as administrator (username *admin*).

The BBI allows you to administer the NSF in the following manner (see Table 1).

Table 1 NSF administration

NSF function	Administration method
Create a configuration	Use the Config functions or Wizards.
Submit form changes	Click **Update** or **Submit** on the form.
View pending changes	Click global **Diff**.
Clear pending changes	Click global **Revert** to cancel all pending changes.
Apply changes	Click global **Apply**.

Up to ten simultaneous browser connections are allowed. When multiple CLI or BBI sessions are open concurrently, only pending changes, made during your current session, are affected by use of the global Diff, Revert, or Logout commands. However, when multiple CLI or BBI administrators apply changes to the same set of parameters concurrently, the latest applied changes take precedence. **TIP**: See Figure 75 on page 107, Administration/Monitor/GUI Lock form. To prevent conflicts, any user logged in as administrator (username *admin*) can take control of the GUI lock before changing or creating a configuration.

Pending change exceptions

After submission, most changes are considered pending and are not immediately put into effect or permanently saved. However, changes to the date or time zone, and users and passwords take effect as soon as the form is submitted. See Cluster/Time/Current Time form on page 40 and Administration/Users/General form on page 110.

Lost changes

Changes are lost if a new form is selected or the session is ended without submitting the information to the pending configuration. Click **Update** or **Submit** on the form to submit changes to the pending configuration.

Pending changes are also discarded if you do not submit them before the inactivity timeout value on BBI sessions elapses. The BBI inactivity timeout value is five minutes and cannot be changed.

Creating a configuration

To create a configuration, do the following:

1) Select the appropriate menu item and subpage.

2) Modify fields in the appropriate forms display areas.

3) Click **Update** to submit the changes to the pending configuration.

Viewing pending changes

To view pending changes before they are applied, do the following:

1) Click global **Diff** .

2) View the global Diff form.

3) Click **Back** to return to the current form.

Clearing pending changes

To clear pending changes, do one of the following:

- Click global **Revert** and return to the configuration. **TIP**: You cannot use the global Revert command to restore the previous configuration after you submit the Apply command.
- Close the browser.

Submitting changes

To submit the form changes for application, do the following:

1) Click global **Apply**. **TIP**: The global Apply command allows updates on multiple forms to be put into effect all at once. The Apply function validates the changes to the configuration before applying them, and Apply fails if invalid settings are used. See Figure 75 on page 107, Administration/Monitor/GUI Lock form. To prevent conflicts, any user logged in as administrator (username *admin*) can take control of the GUI lock before changing or creating a configuration.

2) Click **Submit**.

See Global command forms for details on using Apply, Diff, Revert, and Logout.

Global command forms

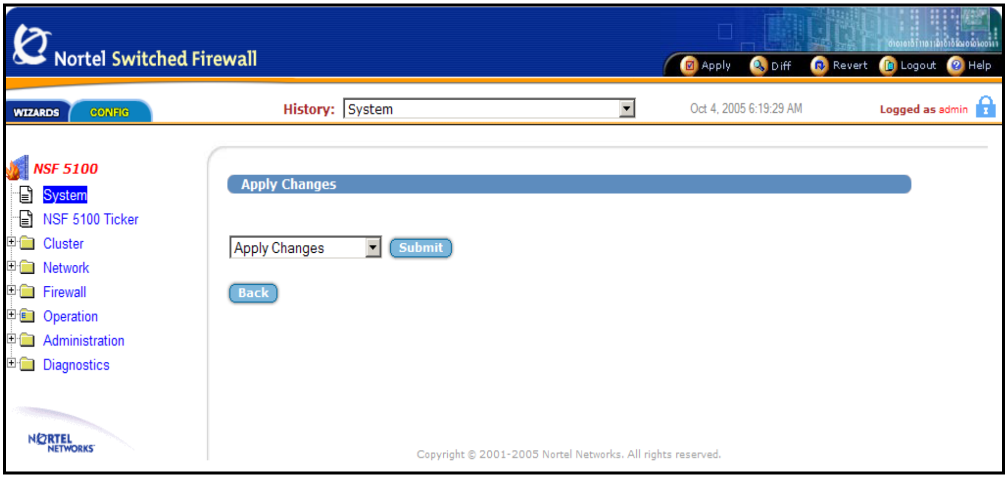
The global command buttons are always available at the top of each form.

These buttons summon forms used to save, examine, or cancel configuration changes, log out, and to display Help information. Each global command form provides options to verify or cancel the command.

Apply Changes

Use the global Apply Changes form to check the validity of the pending configuration changes for the current session, and to save the configuration changes and put them into effect (see Figure 8).

Figure 8 Apply form



History: System

Oct 4, 2005 6:19:29 AM

Logged as admin

Apply Changes

The global Apply form includes the following items:

- Apply Changes list: to use this menu, select one of the following commands and click **Submit**:
  - □ Apply Changes

When selected, this command updates the Nortel Switched Firewall with any pending configuration changes. Pending changes are first validated for correctness (see Validate Configuration on page 25). If no problems are found, the changes are applied and put into effect. If problems are found, applicable warning and error messages are displayed. Warnings are allowed, and the changes are applied and put into effect. Errors are not allowed, and the changes are not applied.

This command has no effect on pending changes in other open CLI or BBI sessions. See Figure 75 on page 107 for information about taking control of the GUI lock.

- □ Validate Configuration

  When selected, this option validates pending changes for the current session, but does not apply them. The pending configuration changes are examined to ensure that they are complete and consistent.

  If problems are found, the following types of messages are displayed:

  Warnings are in yellow. Warnings identify conditions you should consider, but which do not cause errors or prevent configuration application.

  Errors are in red. Errors identify serious configuration problems that require correction. Uncorrected errors cause the Apply Changes command to fail.

  If the configuration is valid, select **Apply Changes** and click **Submit** to apply the changes.

- □ Run a Security Audit

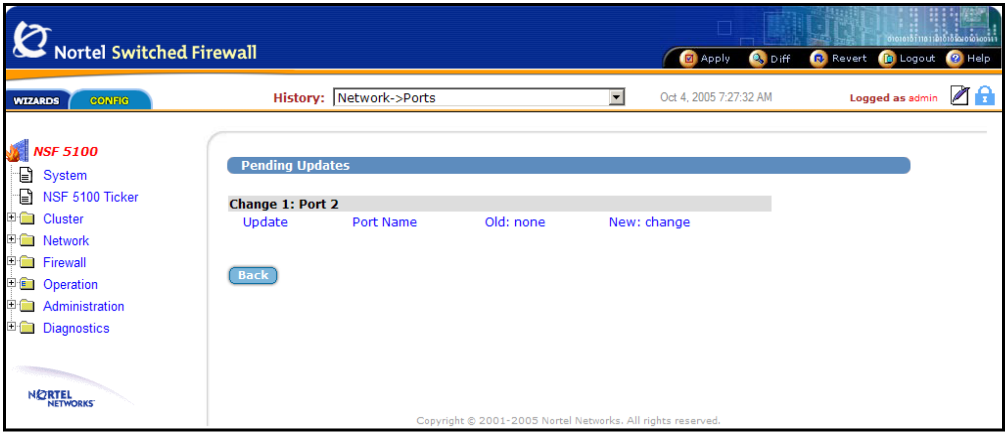
  When selected, this command lists security information. Security information includes the status for remote management features such as Telnet, SSH, and the BBI for the cluster. The IP addresses that access the remote management features are also listed. The Run Security Audit command also lists users configured with default passwords that require change.

- **Submit** button: Click to perform the action selected in the Apply Changes list.
- **Back** button: Click to return to the previously viewed form without applying changes.

Diff

The global Diff command displays the Pending Updates form. Pending Updates provides a list of the pending configuration changes for the current session (see Figure 9).

Figure 9 Diff form



History: Network->Ports

Oct 4, 2005 7:27:32 AM

Logged as admin

Pending Updates

Change 1: Port 2

Update   Port Name   Old: none   New: change

Copyright © 2001-2005 Nortel Networks. All rights reserved.

The list displays a change record for each submitted update. Each record can consist of many modifications, depending upon the complexity of the form and changes submitted. Modifications are color-coded as follows:

- **Green**: New items that will be *added* to the configuration when the global Apply command is given and verified.
- **Blue**: Existing items that will be *modified*.
- **Red**: Configuration items that will be *deleted*.

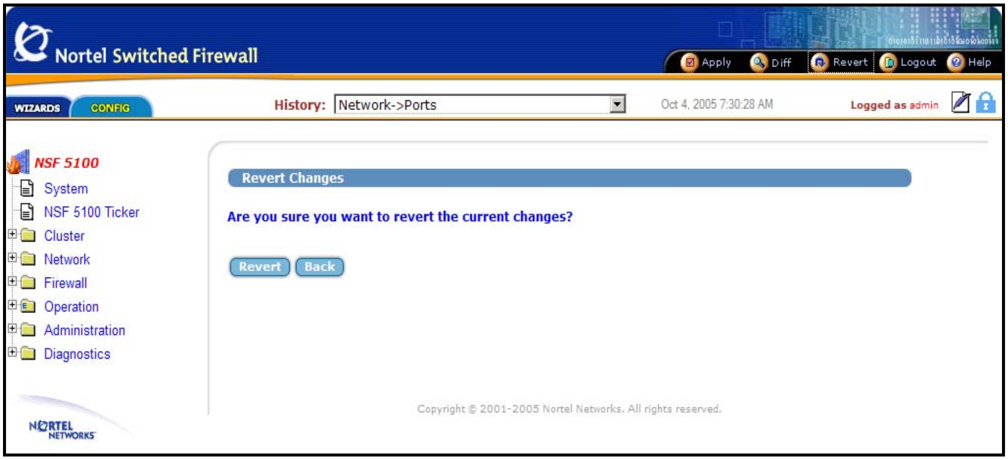
The Diff list is cleared when configuration changes are applied or reverted, or when you log out or close the browser window.

Note – The Diff form does not include pending changes made in other concurrent CLI or BBI sessions.

Revert

The global Revert command displays the Revert Changes form. Use Revert to cancel pending configuration changes (see Figure 10).

Figure 10 Revert form



History: Network->Ports

Oct 4, 2005 7:30:28 AM

Logged as admin

Revert Changes

Are you sure you want to revert the current changes?

Copyright © 2001-2005 Nortel Networks. All rights reserved.

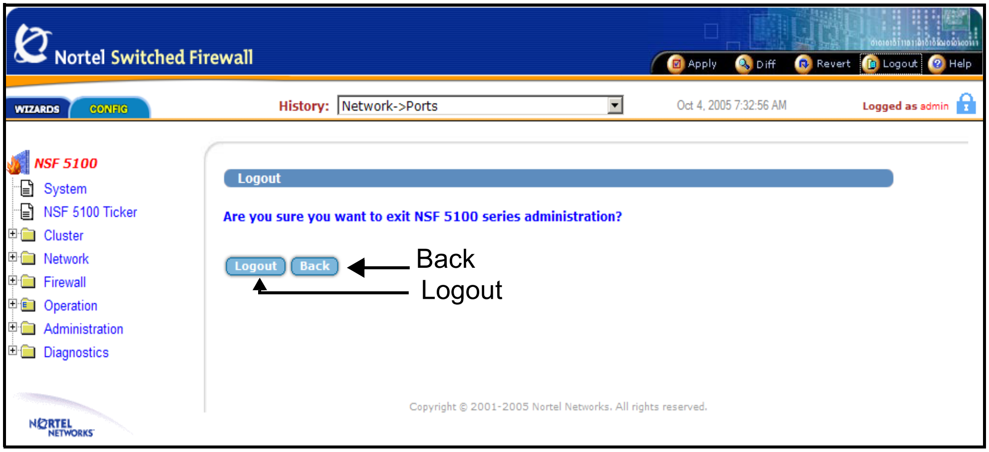
The global Revert form includes the following items:

- Revert button: Click **Revert** to cancel the pending configuration changes for the current session. **TIP**: Applied changes are not affected. Pending changes made in other open CLI or BBI sessions are not affected. See Figure 75 on page 107, Administration/Monitor/GUI Lock form. To prevent conflicts, any user logged in as administrator (username *admin*) can take control of the GUI lock before changing or creating a configuration.
- Back button: Click **Back** to return to the previously viewed form without canceling pending changes.

Logout

Use the global Logout form to terminate the current user session (see Figure 11).

Figure 11 Logout form



History: Network->Ports

Oct 4, 2005 7:32:56 AM

Logged as admin

Logout

Are you sure you want to exit NSF 5100 series administration?

Copyright © 2001-2005 Nortel Networks. All rights reserved.

The global Logout form includes the following items:

- Logout button: Click **Logout** to terminate the current user session. **TIP**: Any configuration changes made during this session that have not been applied are lost. This command has no effect on pending changes in other open CLI or BBI sessions.
- Back button: Click **Back** to return to the previously viewed form without logging out.

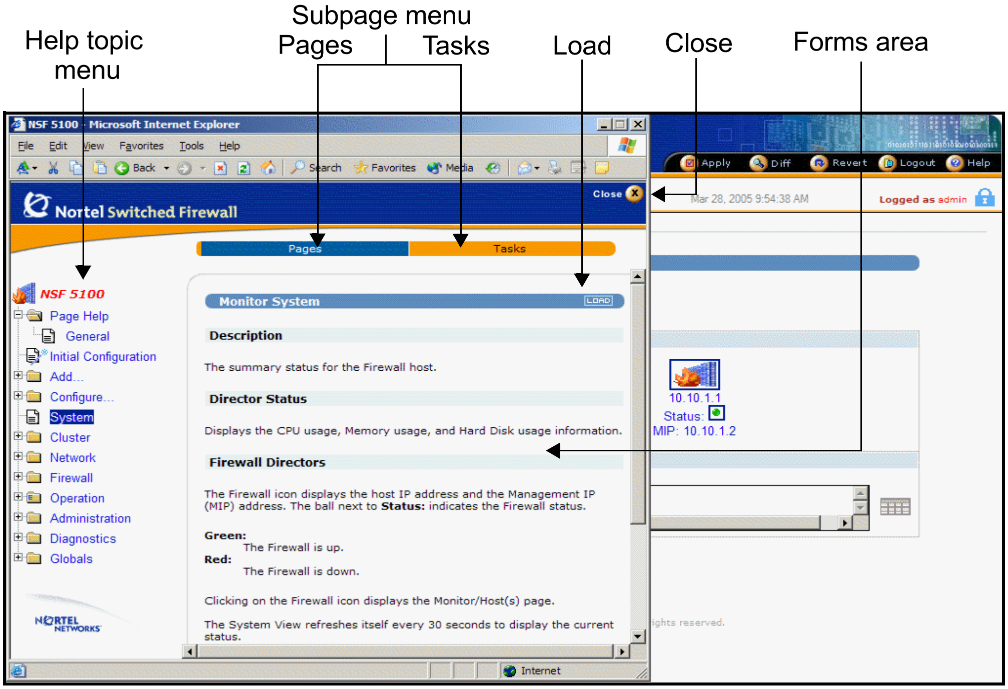
Help

The global Help form provides assistance with forms and tasks in the BBI. Two kinds of Help are available: context-sensitive Help and task-based Help.

Context-sensitive Help

Context-sensitive Help displays detailed information about the currently displayed form in the BBI forms area. Click global **Help** to view a new window showing Help information appropriate to your current options (see Figure 12).

Figure 12 Context-sensitive Help form



Monitor System

Description

The summary status for the Firewall host.

Director Status

Displays the CPU usage, Memory usage, and Hard Disk usage information.

Firewall Directors

The Firewall icon displays the host IP address and the Management IP (MIP) address. The ball next to **Status:** indicates the Firewall status.

Green: The Firewall is up.

Red: The Firewall is down.

Clicking on the Firewall icon displays the Monitor/Host(s) page.

The System View refreshes itself every 30 seconds to display the current status.

The context-sensitive Help window consists of the following areas:

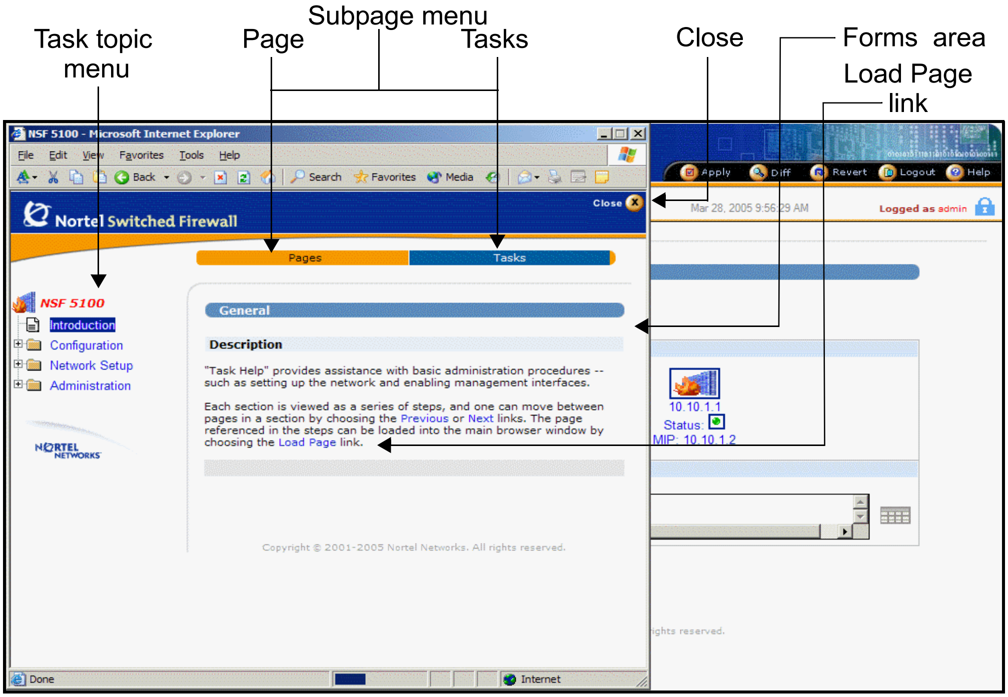
- Subpage menu: Click **Pages** to display Help for the selected form. Click **Tasks** to activate the task-based Help system.
- Help topic menu: Select a new Help topic using the menu on the left side of the Help window. Each main menu item is listed, along with the submenu items under the current selection. Select a different menu item to display its submenu list. Select any submenu item to display Help for that form.
- Load: Click **Load** to display the form referenced on the bar.

- Forms area: This area displays detailed information about the selected topic.
- Close button: Click **Close** to close the context-sensitive Help window.

Task-based Help

Task-based Help directs the administrator through the steps of various common procedures. To access task-based Help, click global **Help** and then click the **Tasks** bar. The task Help menu appears in a new window with information appropriate for the current BBI form (see Figure 13):

Figure 13 Task-based Help form



General

Description

"Task Help" provides assistance with basic administration procedures -- such as setting up the network and enabling management interfaces.

Each section is viewed as a series of steps, and one can move between pages in a section by choosing the Previous or Next links. The page referenced in the steps can be loaded into the main browser window by choosing the Load Page link.

Copyright © 2001-2005 Nortel Networks. All rights reserved.

The task-based Help window consists of the following areas:

- Subpage menu: Click **Pages** to display Help for the selected form. Click **Tasks** to activate the task-based Help system (see Figure 13).
- Task topic menu: Select from a list of tasks using the menu on the left side of the Help window. Each main task item is listed, along with the subtasks under the current selection. Select a different subtask to reveal the steps required to complete it.
- Forms area: This area displays the steps required to complete the selected subtask.

- Load Page link: Click **Load Page** to display the form referenced on the task topic menu. If the subtask has more than one step, the steps are listed on the form.
  - □ Click ▶ to display the information for the next subtask.
  - □ Click ◀ to display the information for the previous subtask.
- Close button: Click **Close** to close the task-based Help window.

CHAPTER 3

Browser-Based Interface forms reference

BBI main menu selections

The following eight selections are available on the Nortel Switched Firewall (NSF) Browser-Based Interface (BBI) Config tab main menu:

- System form on page 34
- NSF 5100 Ticker form on page 34
- Cluster forms on page 38
- Network forms on page 50
- Firewall forms on page 89
- Operation forms on page 97
- Administration forms on page 102
- Diagnostics forms on page 145

Pages, called forms, are available for each menu selection. Use these forms to configure, manage, or obtain information about the NSF BBI.

The following selections are available on the NSF BBI Wizards tab main menu:

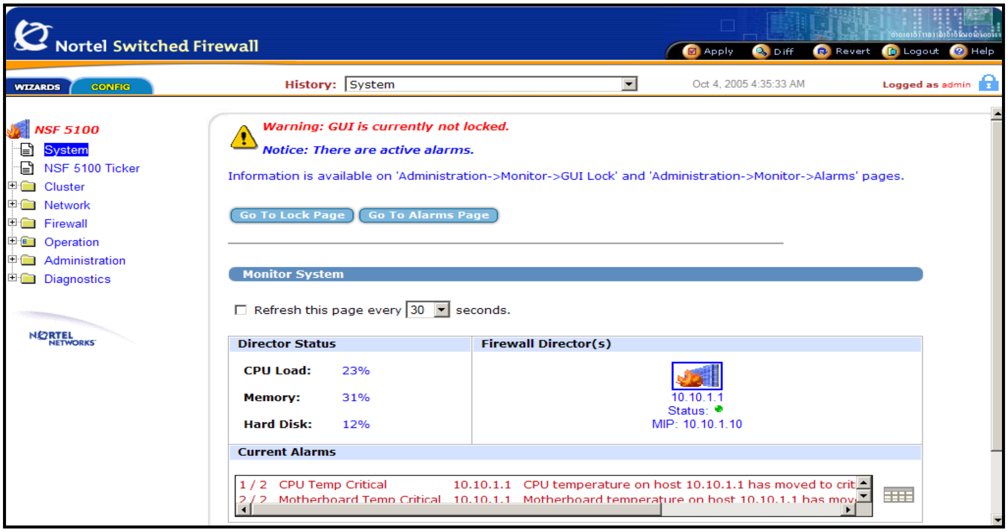
- Initial Configuration
- Add
- Configure

For more information about the Wizards forms, see Wizards forms on page 154.

System form

When you select System, the Main page, also known as the Monitor System form, is displayed as shown in Monitor System form. For more information about the System form, see Interface components on page 17.

Figure 14 Monitor System form



History: System

Oct 4, 2005 4:35:33 AM

Logged as admin

Warning: GUI is currently not locked.

Notice: There are active alarms.

Information is available on 'Administration->Monitor->GUI Lock' and 'Administration->Monitor->Alarms' pages.

□ Refresh this page every 30 seconds.

Director Status		Firewall Director(s)
CPU Load:	23%	10.10.1.1 Status: ● MIP: 10.10.1.10
Memory:	31%	
Hard Disk:	12%	

Current Alarms

```
1 / 2   CPU Temp Critical            10.10.1.1   CPU temperature on host 10.10.1.1 has moved to crit
2 / 2   Motherboard Temp Critical    10.10.1.1   Motherboard temperature on host 10.10.1.1 has mov
```

NSF 5100 Ticker form

NSF 5100 Ticker provides a real-time view of the following Firewall status and statistic information:

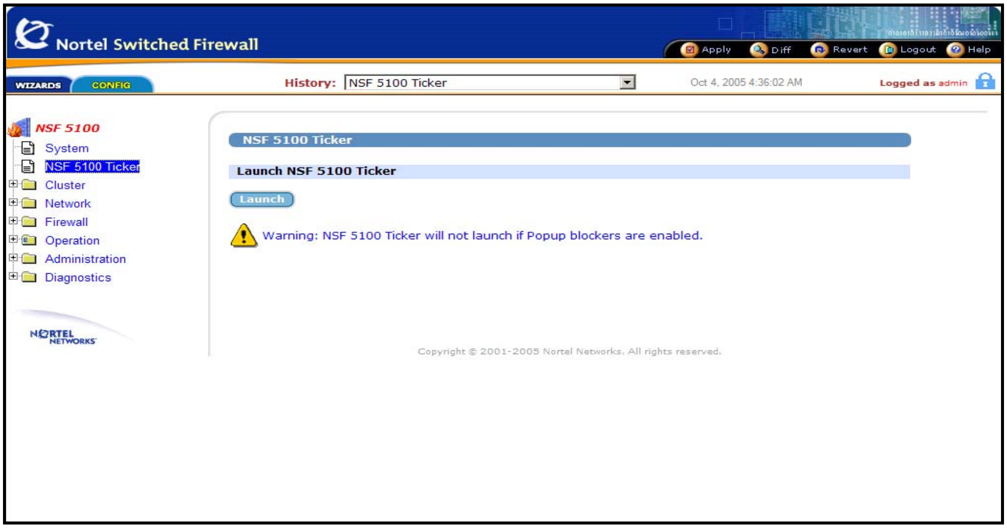
- status of firewall directors and accelerators
- alarms, color coded for status
- statistics for the following parameters:
    - CPU use
    - memory use
    - disk use
    - session statistics plotted as a graph
    - throughput statistics plotted as a graph

- status of the following remote accesses:
    - HTTP
    - HTTPS
    - Telnet
    - SSH
    - SNMP

Use the NSF 5100 Ticker launch form to launch the Ticker. **TIP**: The Ticker cannot launch if pop-up blockers are enabled (see NSF 5100 Ticker launch form).

NOTE – Java 2 Runtime Environment SE plug-in, version 1.2.4-01 or higher, is required. When you launch the Ticker, if the Java plug-in is not present, the Ticker downloads it from the java.sun.com web site. If the system is not connected to the Internet, an error message appears in the Ticker window.

Figure 15 NSF 5100 Ticker launch form



History: NSF 5100 Ticker

Oct 4, 2005 4:36:02 AM

Logged as admin

Warning: NSF 5100 Ticker will not launch if Popup blockers are enabled.

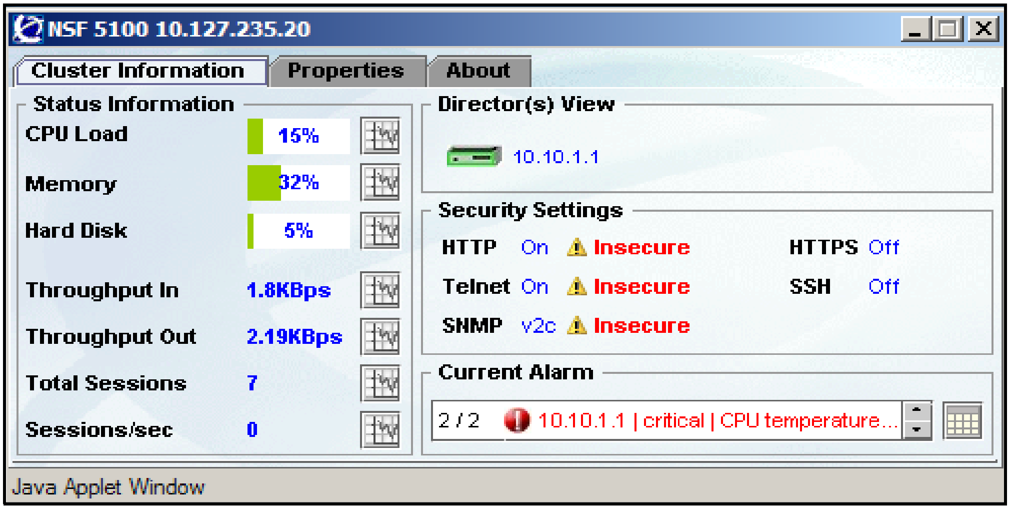
Copyright © 2001-2005 Nortel Networks. All rights reserved.

Click **Launch** on the NSF 5100 Ticker Launch form to launch the Ticker report.

Use the Ticker report form to view the statistics provided by the Ticker.

The NSF 5100 Ticker report form displays three tabs (see NSF 5100 Ticker results form).

Figure 16 NSF 5100 Ticker results form



Status Information

CPU Load 15%

Memory 32%

Hard Disk 5%

Throughput In 1.8KBps

Throughput Out 2.19KBps

Total Sessions 7

Sessions/sec 0

Director(s) View

10.10.1.1

Security Settings

HTTP On ⚠ Insecure HTTPS Off

Telnet On ⚠ Insecure SSH Off

SNMP v2c ⚠ Insecure

Current Alarm

2 / 2 10.10.1.1 | critical | CPU temperature...

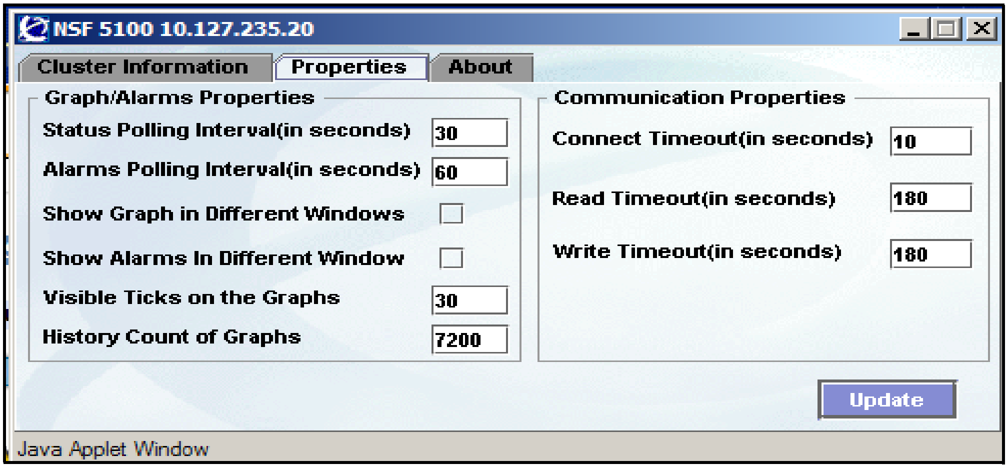
Tabs on the NSF 5100 Ticker results form are as follows:

- Cluster information
- Properties
- About

The Cluster Information page displays the statistics and graphs for the Firewall (see NSF 5100 Ticker results form).

The Properties page displays properties for NSF 5100 Ticker parameters (see NSF 5100 Ticker/Properties form).

Figure 17 NSF 5100 Ticker/Properties form



Graph/Alarms Properties

Status Polling Interval(in seconds) 30

Alarms Polling Interval(in seconds) 60

Show Graph in Different Windows □

Show Alarms In Different Window □

Visible Ticks on the Graphs 30

History Count of Graphs 7200

Communication Properties

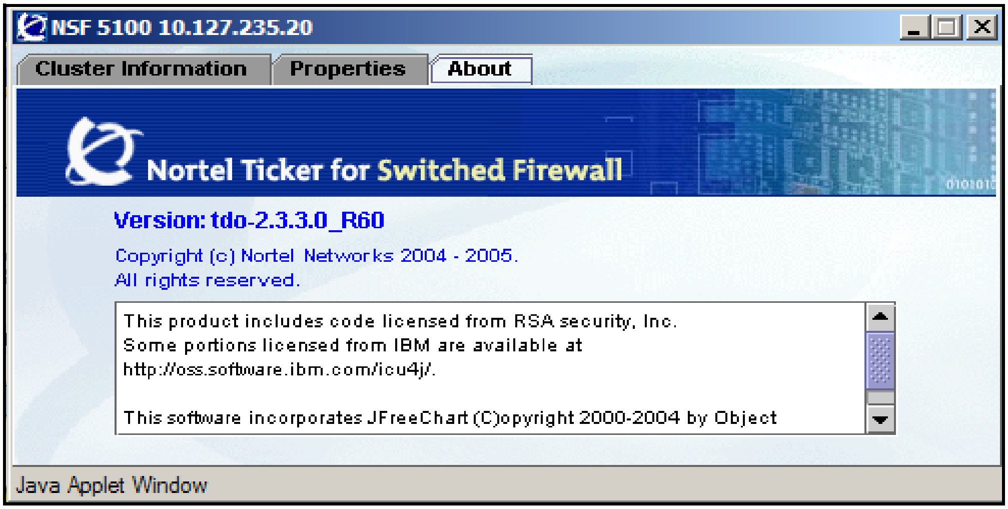
Connect Timeout(in seconds) 10

Read Timeout(in seconds) 180

Write Timeout(in seconds) 180

The About page displays the NSF version and license information (see NSF 5100 Ticker/About form).

Figure 18 NSF 5100 Ticker/About form



Version: tdo-2.3.3.0_R60

Copyright (c) Nortel Networks 2004 - 2005.
All rights reserved.

This product includes code licensed from RSA security, Inc.
Some portions licensed from IBM are available at
http://oss.software.ibm.com/icu4j/.

This software incorporates JFreeChart (C)opyright 2000-2004 by Object

Cluster forms

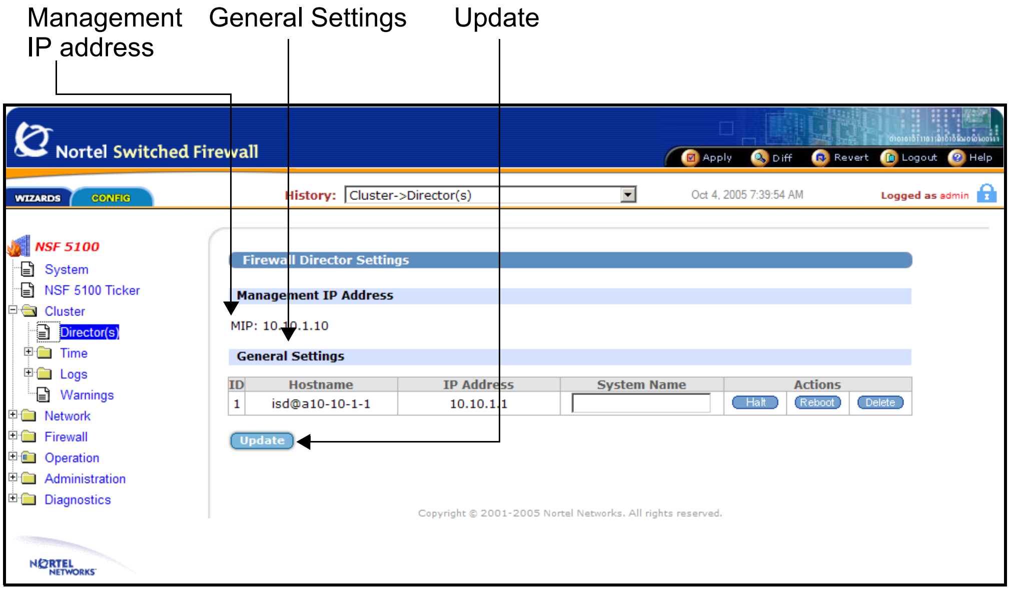
The Cluster menu includes the following categories of forms:

- Director(s) form
- Time forms
  - Current Time (see Cluster/Time/Current Time form on page 40)
  - NTP servers (see Cluster/Time/NTP Servers on page 41)
- Logs
  - Syslog (see Cluster/Logs/Syslog form on page 42)
  - ELA (see Cluster/Logs/ELA form on page 45)
  - Archive (see Cluster/Logs/Archive form on page 47)
- Warnings (see Cluster/Warnings form on page 49)

Director(s) form

Use the Cluster/Director(s) form to view and change the Firewall Director Settings (see Cluster/Director(s) form).

Figure 19 Cluster/Director(s) form



Management IP address

General Settings

Update

Firewall Director Settings

Management IP Address

MIP: 10.10.1.10

General Settings

ID	Hostname	IP Address	System Name	Actions		
1	isd@a10-10-1-1	10.10.1.1		Halt	Reboot	Delete

Update

Copyright © 2001-2005 Nortel Networks. All rights reserved.

The Cluster/Director(s) form is divided into the following two sections:

- Management IP Address
- General Settings

Fields and buttons on the Cluster/Director(s) form are as follows:

- Management IP Address
  - MIP is the Management IP for the host. MIP address identifies the cluster and must be unique on the network.
- General Settings
  - ID is the host identification number.
  - Hostname displays the name of the Firewall host.
  - IP Address is the network IP address for the host.
  - System Name is the set system name.
  - Actions provides the following three options:
    - Click **Halt** to stop the Firewall. TIP: Always click **Halt** before turning the device off.
    - Click **Reboot** to reboot the Firewall.
    - Click **Delete** to delete the member (host) and reset the configuration to factory default settings.
  - Click **Update** to submit changes to the pending configuration.

Time forms

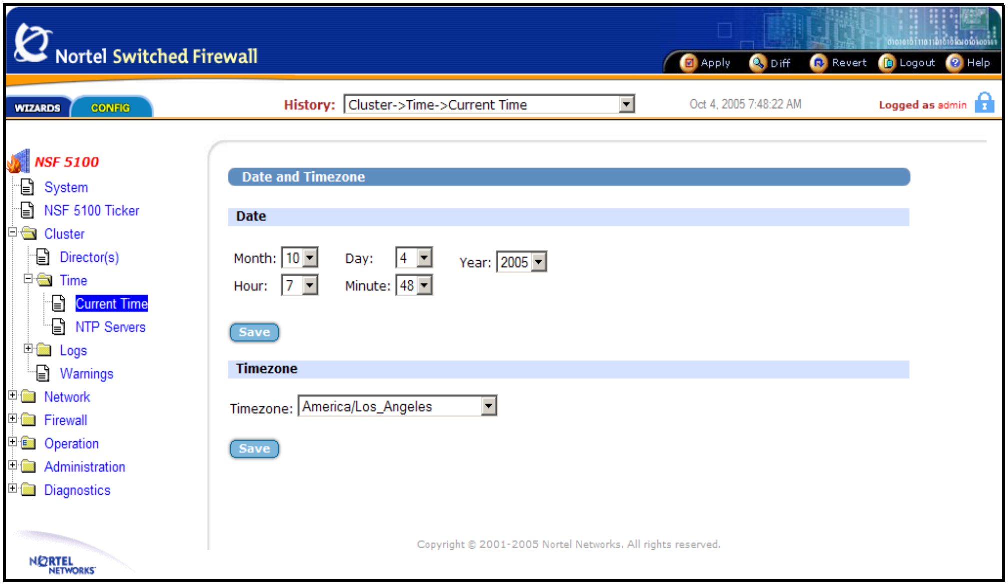
The two Cluster/Time forms are as follows:

- Cluster/Time/Current Time (see Cluster/Time/Current Time form)
- Cluster/Time/NTP Servers (see Cluster/Time/NTP Servers form on page 41)

Cluster/Time/Current Time form

Use the Cluster/Time/Current Time form to set the date and time for the cluster (see Cluster/Time/Current Time form).

Figure 20 Cluster/Time/Current Time form



History: Cluster->Time->Current Time

Oct 4, 2005 7:48:22 AM

Logged as admin

Date and Timezone

Date

Month: 10 Day: 4 Year: 2005

Hour: 7 Minute: 48

Timezone

Timezone: America/Los_Angeles

Copyright © 2001-2005 Nortel Networks. All rights reserved.

The Cluster/Time/Current Time form is divided into the following two sections:

- Date
- Timezone

Fields and buttons on the Cluster/Time/Current Time form are as follows:

- Date fields
  - Month provides a list to select the current month.
  - Day provides a list to select the current date.
  - Year provides a list to select the current year.

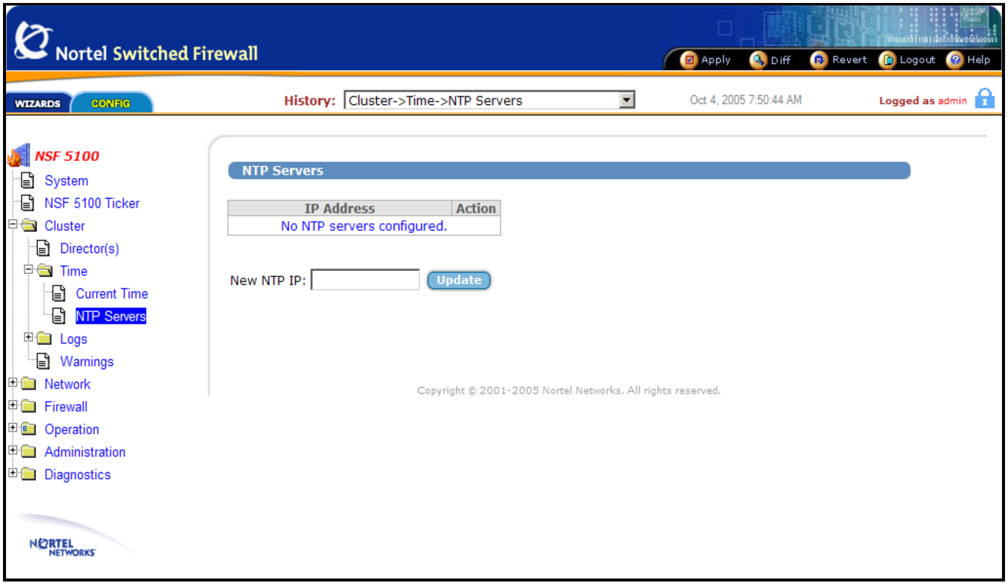
- □ Hour provides a list to select the current hour.
- □ Minute provides a list to select the current minute.

- Click **Save** to submit the date and time changes and to put the changes into immediate effect. Note that changes to the date and time zone are unlike most changes; they are not considered pending after submission.
- Timezone provides a list to select the region.
- Click **Save** to submit the time zone changes and to put the changes into immediate effect. Note that changes to the date and time zone are unlike most changes; they are not considered pending after submission.

Cluster/Time/NTP Servers form

Use the Cluster/Time/NTP Servers form to specify the Network Time Protocol (NTP) servers (see Cluster/Time/NTP Servers).

Figure 21 Cluster/Time/NTP Servers



NTP Servers

IP Address	Action
No NTP servers configured.	

New NTP IP: [ ] Update

NTP servers are used by the NTP client on the NSF to synchronize its clock. The system should have access to at least three servers to compensate for discrepancies between the servers.

Fields and buttons on the Cluster/Time/NTP Servers form are as follows:

- IP Address displays the IP address of an NTP server.
- Action—if an NTP server is present, a Delete button appears.
  - Click **Delete** to delete the server.
- New NTP IP provides a field to configure a new NTP server. **TIP**: Use dotted decimal notation.
- Update submits the NTP server address changes to the pending configuration.

Logs forms

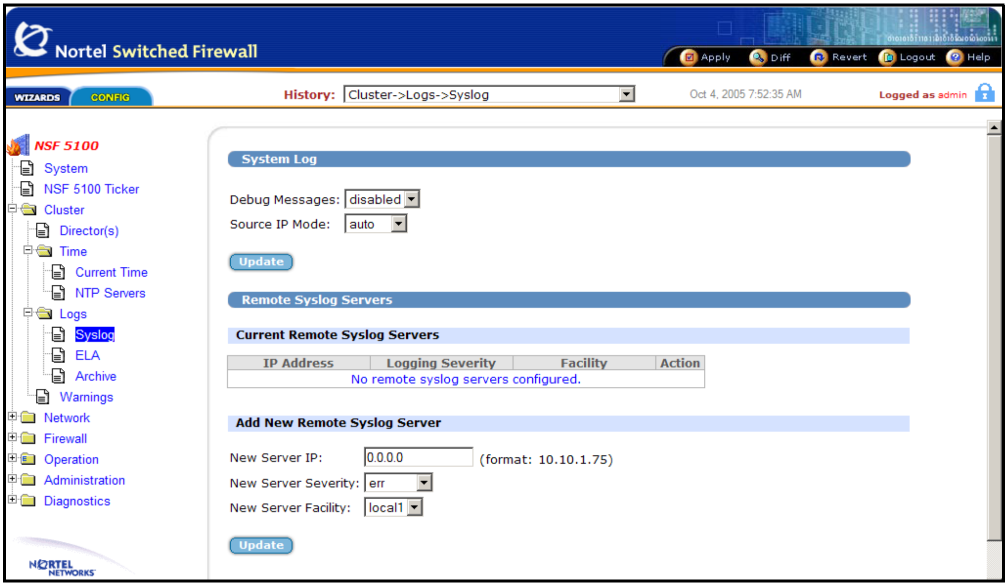
The three Cluster/Logs forms are as follows:

- Syslogs (see Cluster/Logs/Syslog form)
- ELA (see Cluster/Logs/ELA form on page 45)
- Archive (see Cluster/Logs/Archive form on page 47)

Cluster/Logs/Syslog form

Use the Cluster/Logs/Syslog form to specify remote system log servers and turn on local log debugging (see Cluster/Logs/Syslog form).

Figure 22 Cluster/Logs/Syslog form



History: Cluster->Logs->Syslog

System Log

Debug Messages: disabled

Source IP Mode: auto

Remote Syslog Servers

Current Remote Syslog Servers

IP Address	Logging Severity	Facility	Action
No remote syslog servers configured.			

Add New Remote Syslog Server

New Server IP: 0.0.0.0 (format: 10.10.1.75)

New Server Severity: err

New Server Facility: local1

Fields and buttons on the Cluster/Logs/Syslog form are as follows:

System Log

- Debug Messages displays a list with two choices.
  - Disabled disables transmission of debug messages to the local system log.
  - Enabled enables transmission of debug messages to the local system log.
- Source IP Mode displays a list with three choices.
  - Auto, the default setting, specifies the IP address of the outgoing interface.
  - Unique specifies the IP address of the individual NSF.
  - MIP specifies the IP address of the cluster MIP. Use this setting with applications designed for devices limited to one IP address (for example, some versions of HP OpenView).
- Update submits the debug message status change and the source IP mode change to the pending configuration.

The Remote Syslog Servers section of the Cluster/Logs/Syslog form is divided into the following two sections:

- Current Remote Syslog Servers
- Add New Remote Syslog Server

Current Remote Syslog Servers displays the following fields:

- IP Address specifies the remote syslog server in dotted decimal notation.
- Logging Severity specifies the severity of messages logged. All messages of the selected severity or higher are logged.
- Facility provides the local facility number used to uniquely identify syslog entries.
- Action—Click **Delete** to delete an active remote server.

Add New Remote Syslog Server displays the following fields:

- New Server IP specifies the IP address for the remote syslog server. **TIP**: Enter the IP address in dotted decimal notation.
- New Server Severity specifies the severity of messages logged. The following selections are presented in the list:
  - emerg
  - alert

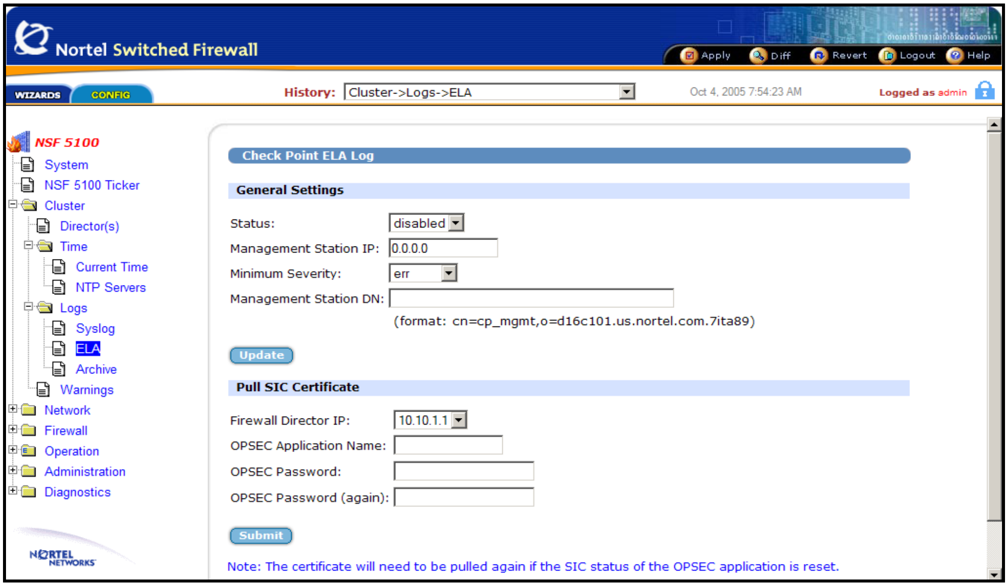
  - crit
  - err
  - warning
  - notice
  - info
  - debug
- New Server Facility provides a list with the following local facility numbers used to uniquely identify syslog entries:
  - auto
  - local0
  - local1
  - local2
  - local3
  - local4
  - local5
  - local6
  - local7
- Click **Update** to submit the Remote Syslog Server changes to the pending configuration.

Cluster/Logs/ELA form

Use the Cluster/Logs/ELA form to configure Event Logging API (ELA) (see Cluster/Logs/ELA form).

ELA allows Firewall log messages to be sent to a Check Point SmartCenter Server for display through the Check Point SmartView Tracker.

Figure 23 Cluster/Logs/ELA form



History: Cluster->Logs->ELA   Oct 4, 2005 7:54:23 AM   Logged as admin

Check Point ELA Log

General Settings

Status: disabled

Management Station IP: 0.0.0.0

Minimum Severity: err

Management Station DN:

(format: cn=cp_mgmt,o=d16c101.us.nortel.com.7ita89)

Pull SIC Certificate

Firewall Director IP: 10.10.1.1

OPSEC Application Name:

OPSEC Password:

OPSEC Password (again):

Note: The certificate will need to be pulled again if the SIC status of the OPSEC application is reset.

NOTE – Configure an ELA service on the Check Point management station and transfer a SIC Certificate for the service to the Firewall to enable ELA logging. For configuration details, see the *Nortel Switched Firewall 2.3.3 User's Guide and Command Reference,* (213455-L).

The Cluster/Logs ELA (Check Point ELA Log) form is divided into the following two sections:

- General Settings
- Pull SIC Certificate

General Settings displays the following fields:

- Status displays a list with two choices:
  - □ Disabled disables Check Point ELA logging.
  - □ Enabled enables Check Point ELA logging.

- Management Station IP provides an entry field to specify the IP address of the Check Point SmartCenter Server where the Firewall log messages are sent.
- Minimum Severity provides a list that specifies the severity of messages logged and sent to the ELA service.
  - emerg
  - alert
  - crit
  - err
  - warning
  - notice
  - info
  - debug
- Management Station DN is the designated name of the Check Point SmartCenter Server.
- Update submits the form changes to the pending configuration.

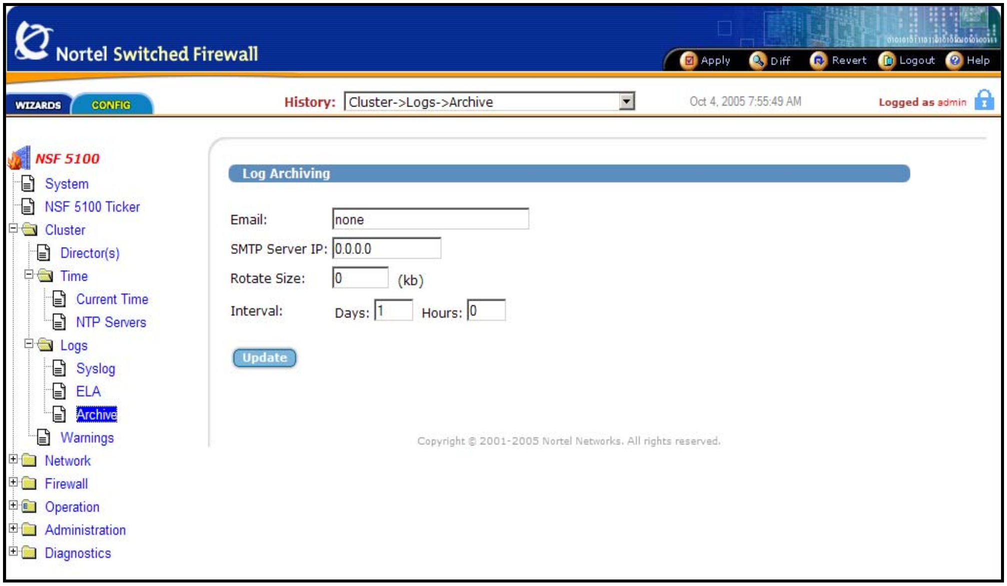
Pull SIC Certificate displays the following fields:

- Firewall Director IP provides a list to specify the IP address of the individual Firewall for update. **TIP**: Do not use the MIP address.
- OPSEC Application Name is the name of the ELA service configured on the Check Point SmartCenter Server. Use the name specified when creating the OPSEC application in the Check Point SmartDashboard. **TIP**: Use a different OPSEC application for each Firewall.
- OPSEC Password is the password used to configure the ELA service on the Check Point Management Station.
- OPSEC Password (again) is used to verify the password.
- Submit is used to submit the form and update the certificate on the specified Firewall.

Cluster/Logs/Archive form

Use the Cluster/Logs/Archive form to specify system log rotation and system log archiving parameters (see Cluster/Logs/Archive form).

Figure 24 Cluster/Logs/Archive form



History: Cluster->Logs->Archive

Email: none

SMTP Server IP: 0.0.0.0

Rotate Size: 0 (kb)

Interval: Days: 1 Hours: 0

Fields and buttons on the Cluster/Logs/Archive form are as follows:

- Email specifies an e-mail address for the administrator receiving the log.
- SMTP Server IP specifies the IP address of the SMTP server in dotted decimal notation. **TIP**: The SMTP Server must be configured to accept messages from the Firewall and a Check Point policy must be present to allow these messages through the Firewall.
- Rotate Size specifies the maximum size the log reached before rotation. If this parameter is set at 0, then the size is ignored and only the log rotate interval is used.
- Interval specifies, in days and hours, the interval at which the system log file is rotated.
- Update submits the form changes to the pending configuration.

Log file rotation

Log files are rotated when the file reaches a specific size or age.

If the log file rotate size is set to 0, the file size is ignored and the rotate interval is used to determine log rotation. **TIP**: Set the rotate interval in days and hours.

If the log file rotate size is set to >0, log rotation occurs when one of the following conditions is met:

- The log file surpasses the rotate size.
- The log file rotation interval is reached.

Rotated log files are managed in one of the following ways when rotation occurs:

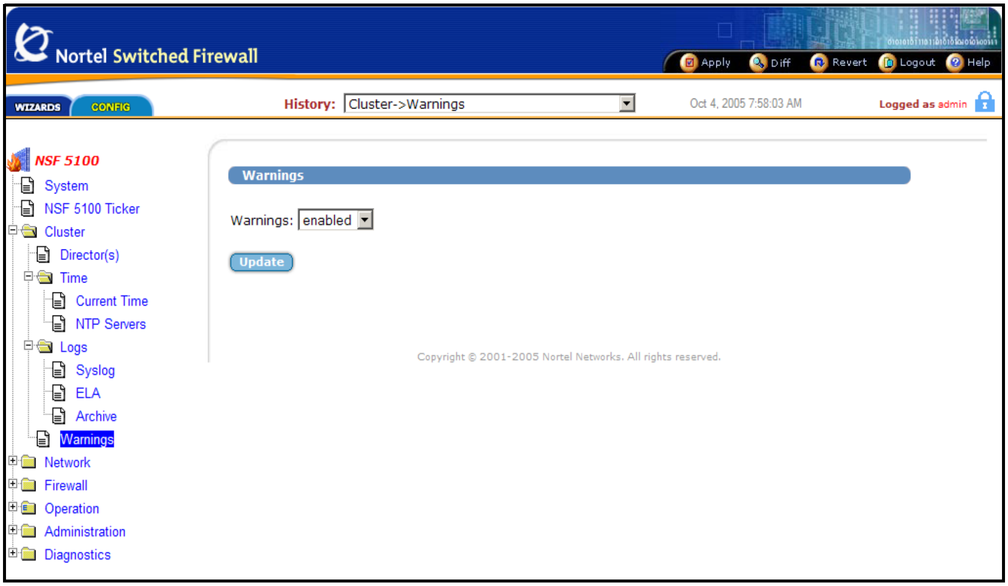
- The rotated log file is set aside.
- The rotated log file is e-mailed. **TIP**: Specify an e-mail address and SMTP server IP address.

When the log file is rotated, a new log file is started.

Warnings form

Use the Cluster/Warnings form to enable or disable configuration warning messages (see Cluster/Warnings form).

Figure 25 Cluster/Warnings form



History: Cluster->Warnings

Warnings: enabled

Fields and buttons on the Cluster/Warnings form are as follows:

- Warnings displays a list with two selections.
    - Disabled disables the display of warning messages about the state of pending configuration changes when the global Apply command is issued.
    - Enabled enables the display of warning messages about the state of pending configuration changes when the global Apply command is issued.
- Update submits the Warning selection to the pending configuration.

Network forms

The Network menu includes the following categories of forms:

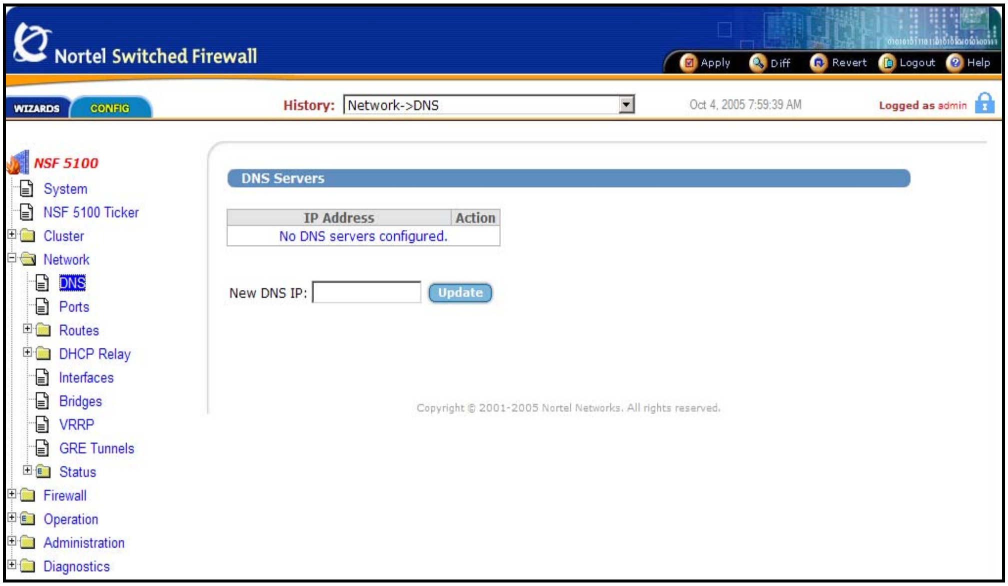
- DNS (see Network/DNS form on page 51)
- Ports (see Network/Ports form on page 52)
- Routes
  - Static (see Network/Routes/Static form on page 54)
  - Proxy ARP (see Network/Routes/Proxy ARP form on page 57)
  - Gateway (see Network/Routes/Gateway form on page 58)
  - OSPF
    - General (see Network/Routes/OSPF/General form on page 59)
    - Area Indexes (see Network/Routes/OSPF/Area Indexes form on page 60)
    - Interfaces (see Network/Routes/OSPF/Interfaces form on page 62)
    - GRE Tunnels (see Network/Routes/OSPF/GRE Tunnels form on page 64)
    - Redistribute (see Network/Routes/OSPF/Redistribute form on page 67)
- DHCP Relay
  - General (see Network/DHCP Relay/General form on page 69)
  - Interfaces (see Network/DHCP Relay/Interfaces form on page 70)
  - Servers (see Network/DHCP Relay/Servers form on page 72)
- Interfaces (see Network/Interfaces form on page 74)
- Bridges (see Network/Bridges form on page 78)
- VRRP (see Network/VRRP form on page 80)
- GRE Tunnels (see Network/GRE Tunnels form on page 82)
- Status
  - Interface (see Network/Status/Interface form on page 85)
  - Link (see Network/Status/Link form on page 86)
  - Bridge Statistics (see Network/Status/Bridge Statistics form on page 87)
  - Bridge Mac Entries (see Network/Status/Bridge Mac Entries form on page 88)

NOTE – The NSF provides administrators with the option to configure Layer 2 and Layer 3 firewalls. The Layer 2 and Layer 3 firewall configuration procedures differ only in the configuration of the IP addresses. A Layer 3 firewall requires valid IP addresses for address 1 and address 2. A Layer 2 firewall requires no IP addresses. For detailed Layer 2 and Layer 3 configuration, see *Nortel Switched Firewall 2.3.3 User's Guide and Command Reference,* (213455-L).

DNS form

Use the Network/DNS form to specify the Domain Name Service (DNS) servers. Multiple servers are allowed (see Network/DNS form).

Figure 26 Network/DNS form



History: Network->DNS

Oct 4, 2005 7:59:39 AM

Logged as admin

DNS Servers

IP Address	Action
No DNS servers configured.	

New DNS IP:

Copyright © 2001-2005 Nortel Networks. All rights reserved.

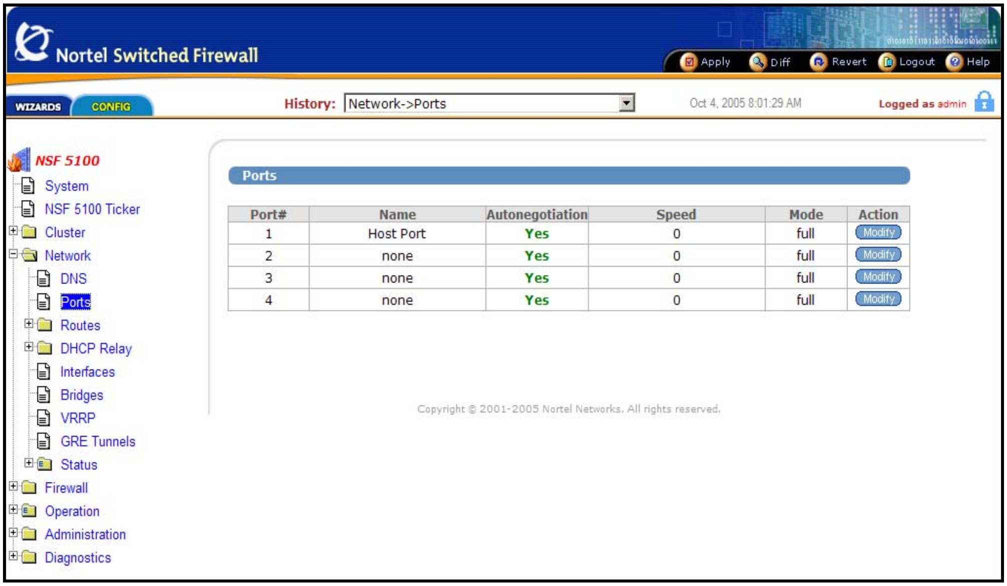
Fields and buttons on the Network/DNS form are as follows:

- IP Address specifies the IP address of a configured DNS server.
- Action displays a Delete button if a DNS server is present.
- New DNS IP provides an entry field to specify a new DNS server address. **TIP**: Use dotted decimal notation.
- Update submits the DNS server address changes to the pending configuration.

Ports form

Use the Network/Ports form to configure network port settings (see Network/Ports form).

Figure 27 Network/Ports form



History: Network->Ports

Oct 4, 2005 8:01:29 AM

Logged as admin

Ports

Port#	Name	Autonegotiation	Speed	Mode	Action
1	Host Port	Yes	0	full	Modify
2	none	Yes	0	full	Modify
3	none	Yes	0	full	Modify
4	none	Yes	0	full	Modify

Copyright © 2001-2005 Nortel Networks. All rights reserved.

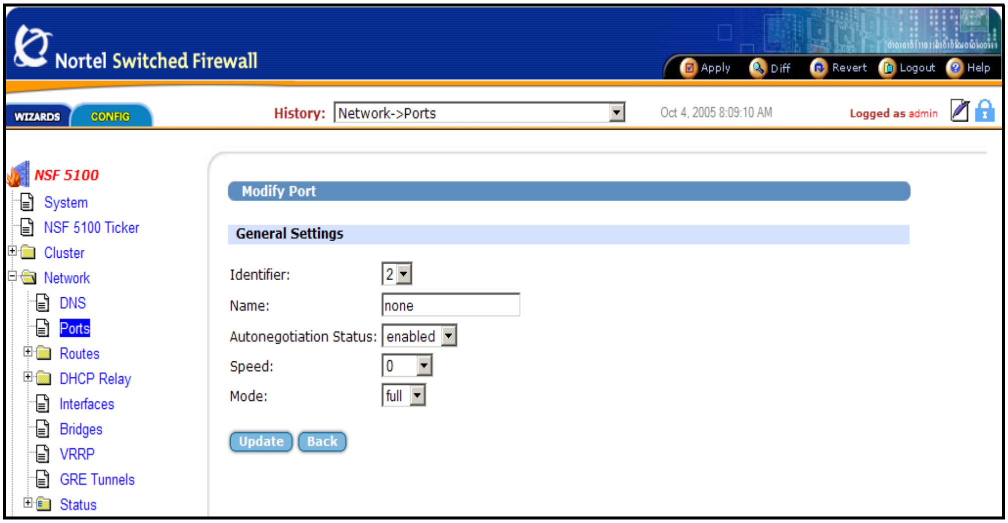
Fields and buttons on the Network/Ports form are as follows:

- Port# specifies the port number on the Firewall.
- Name provides the name of the port.
- Autonegotiation provides two choices:
  - Yes indicates that autonegotiation is enabled.
  - No indicates that autonegotiation is disabled.
- Speed specifies the port data rate, in Mbps, of 0, 10, 100, or 1000. **TIP**: Port speed is not applicable if autonegotiation is enabled.
- Mode provides two duplex options:
  - Half
  - Full
- Action provides the option to modify a form and update port settings (see Network/Ports Modify Port formFigure 28 on page 53).

Network/Ports Modify Port form

Use the Network/Ports Modify Port form to modify the settings for a selected port.

Figure 28 Network/Ports Modify Port form



History: Network->Ports

Modify Port

General Settings

Identifier:	2
Name:	none
Autonegotiation Status:	enabled
Speed:	0
Mode:	full

The following fields can be modified on the Network/Ports Modify Port form:

- Identifier provides an entry field for a port number. **TIP**: Select a number between 1 and 6.
- Name provides an entry field to specify a name for the port.
- Autonegotiation Status provides a list with the following two selections:
  - Enabled enables port autonegotiation. **TIP**: Port speed setting is ignored if autonegotiation is enabled.
  - Disabled disables port autonegotiation.
- Speed provides a list with the following selections:
  - 0 Mbps
  - 10 Mbps
  - 100 Mbps
  - 1000 Mbps

- Mode provides for following two selections:
  - □ Half (duplex)
  - □ Full (duplex)
- Update submits the port changes to the pending configuration.
- Back returns to the Network/Ports form without submitting changes to the pending configuration.

Routes forms

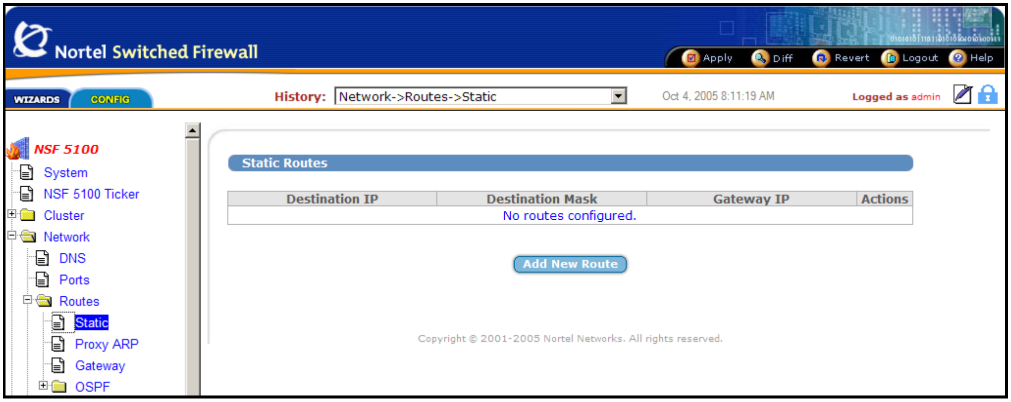
Following are the four main categories of forms in the Network/Routes menu:

- Static (see Network/Routes/Static form)
- Proxy ARP (see Network/Routes/Proxy ARP form on page 57)
- Gateway (see Network/Routes/Gateway form on page 58)
- OSPF (see Network/Routes/OSPF/General form on page 59)

Network/Routes/Static form

Use the Network/Routes/Static form to view and configure static routes on the Firewall (see Network/Routes/Static form).

Figure 29 Network/Routes/Static form



Static Routes

Destination IP	Destination Mask	Gateway IP	Actions
No routes configured.			

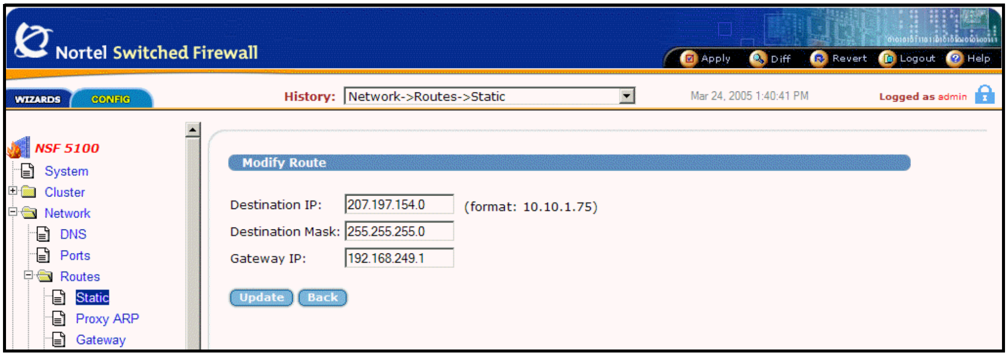
Fields and buttons on the Network/Routes/Static form are as follows:

- Destination IP specifies the IP address of the route destination. **TIP**: Use dotted decimal notation.
- Destination Mask specifies the subnet mask for the route destination. **TIP**: Use dotted decimal notation.
- Gateway IP specifies the IP address of the gateway. **TIP**: Use dotted decimal notation.
- Actions provides two choices, which are visible only if routes are present:
  - Delete, to delete a route from the system.
  - Modify, to modify the parameters of a displayed route (see Network/Routes/Static Modify Route form).
- Add New Route adds a new route to the configuration (see Network/Routes/Static Add Route form on page 56).

Network/Routes/Static Modify Route form

Use the Network/Routes/Static Modify Route form to modify the parameters of a displayed route.

Figure 30 Network/Routes/Static Modify Route form



History: Network->Routes->Static

Destination IP: 207.197.154.0 (format: 10.10.1.75)

Destination Mask: 255.255.255.0

Gateway IP: 192.168.249.1

Fields and buttons on the Network/Routes/Static Modify Route form are as follows:

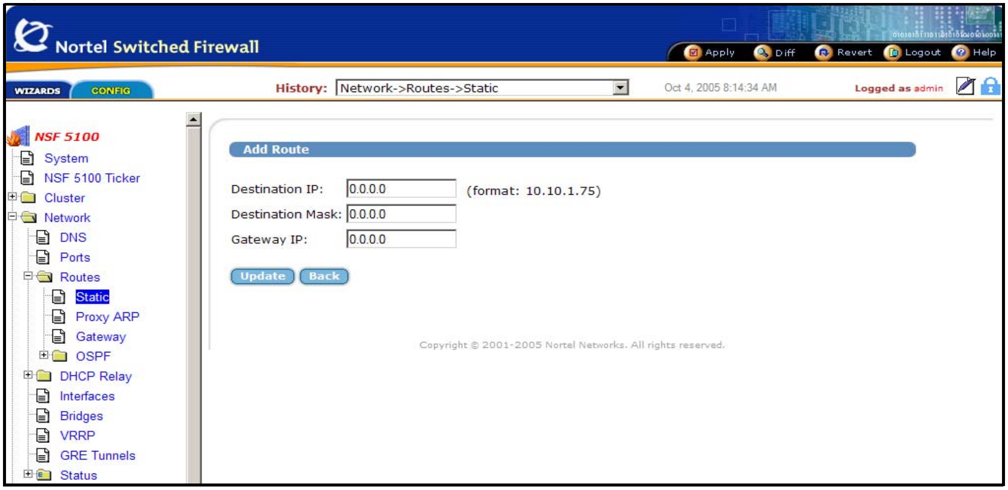
- Destination IP specifies the IP address of the route destination. **TIP**: Use dotted decimal notation.
- Destination Mask specifies the subnet mask for the route destination. **TIP**: Use dotted decimal notation.
- Gateway IP specifies the IP address of the gateway. **TIP**: Use dotted decimal notation.
  - Update submits the changes to the pending configuration.

- Back returns to the Network/Routes/Static form without submitting changes to the pending configuration.

Network/Routes/Static Add Route form

Use the Network/Routes/Static Add Route form to add a new static route to the configuration.

Figure 31 Network/Routes/Static Add Route form



Add Route

Destination IP: 0.0.0.0 (format: 10.10.1.75)

Destination Mask: 0.0.0.0

Gateway IP: 0.0.0.0

History: Network->Routes->Static

Oct 4, 2005 8:14:34 AM

Logged as admin

Copyright © 2001-2005 Nortel Networks. All rights reserved.

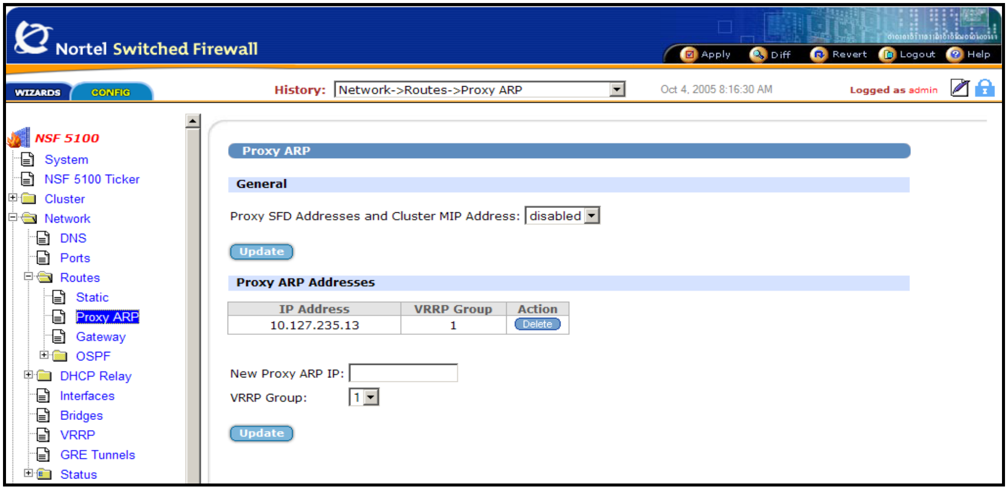
Fields and buttons on the Network/Routes/Static Add Route form are as follows:

- Destination IP specifies the IP address of the route destination. **TIP**: Use dotted decimal notation.
- Destination Mask specifies the subnet mask for the route destination. **TIP**: Use dotted decimal notation.
- Gateway IP specifies the IP address of the gateway. **TIP**: Use dotted decimal notation.
- Update submits the changes to the pending configuration.
- Back returns to the Network/Routes/Static form without submitting changes to the pending configuration.

Network/Routes/Proxy ARP form

Use the Network/Routes/Proxy ARP (Address Resolution Protocol) form to view and configure the Proxy ARP status and addresses that allow the Firewall to respond to Proxy ARP requests (see Network/Routes/Proxy ARP form).

Figure 32 Network/Routes/Proxy ARP form



History: Network->Routes->Proxy ARP

Oct 4, 2005 8:16:30 AM

Logged as admin

Proxy ARP

General

Proxy SFD Addresses and Cluster MIP Address: disabled

Proxy ARP Addresses

IP Address	VRRP Group	Action
10.127.235.13	1	Delete

New Proxy ARP IP:

VRRP Group: 1

The Network/Routes/Proxy ARP form is divided into the following two sections:

- General
- Proxy ARP Addresses

Fields and buttons on the form are as follows:

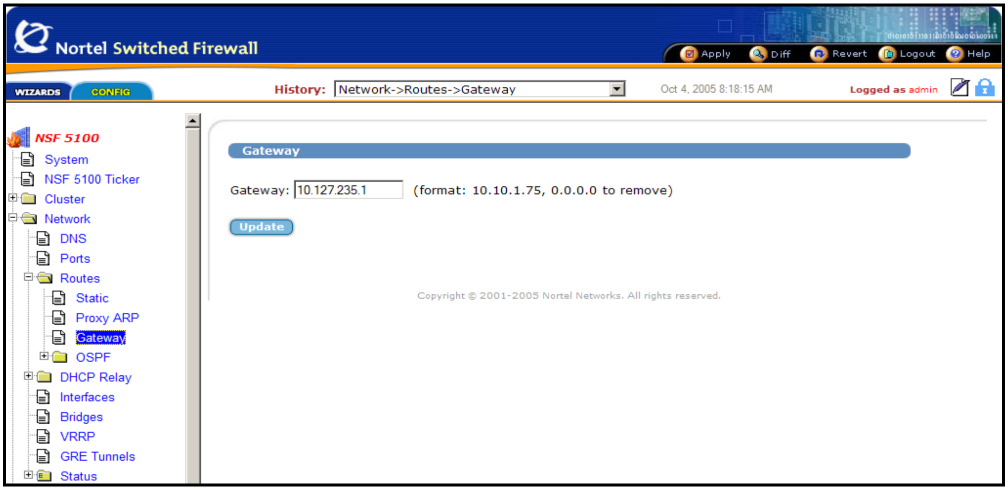
- General
  - Proxy Status contains a list displaying the following selections:
    - Disabled disables Proxy ARP for the cluster.
    - Enabled enables Proxy ARP for the cluster.
  - Update submits the Proxy status change to the pending configuration.
- Proxy ARP Addresses
  - IP Address lists the IP addresses for which the Proxy provides ARPs in the cluster.
  - VRRP Group lists the VRRP group, if VRRP is set up, for which the Proxy provides ARPs in the cluster.
  - Action provides the delete selection used to delete the IP address if at least one Proxy ARP address is present.

- New Proxy ARP IP provides an entry field to specify an IP address. **TIP**: Use dotted decimal format.
- VRRP Group provides a list for VRRP group 1 or 2 selection.
- Update submits the IP address changes to the pending configuration.

Network/Routes/Gateway form

Use the Network/Routes/Gateway form to specify the default gateway for the Firewall (see Network/Routes/Gateway form).

Figure 33 Network/Routes/Gateway form



History: Network->Routes->Gateway

Gateway: 10.127.235.1 (format: 10.10.1.75, 0.0.0.0 to remove)

Fields and buttons on the Network/Routes/Gateway form are as follows:

- Gateway provides an entry field to configure the gateway for the system. **TIP**: Use dotted decimal notation.
- Update submits the form changes to the pending configuration.

Network/Routes/OSPF forms

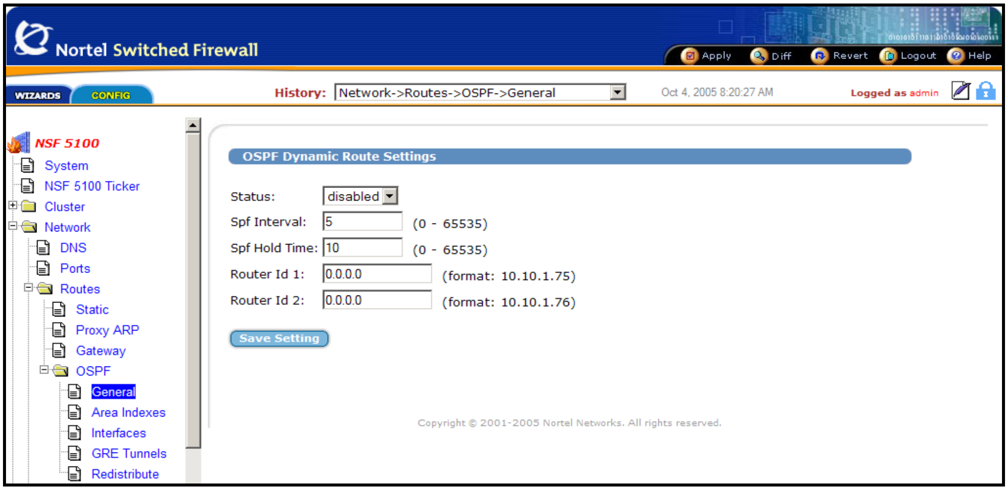
Following are the categories of Network/Routes/OSPF forms:

- General (see Network/Routes/OSPF/General form)
- Area Indexes (see Network/Routes/OSPF/Area Indexes form on page 60)
- Interfaces (see Network/Routes/OSPF/Interfaces form on page 62)
- GRE Tunnels (see Network/Routes/OSPF/GRE Tunnels form on page 64)
- Redistribute (see Network/Routes/OSPF/Redistribute form on page 67)

Network/Routes/OSPF/General form

Use the Network/Routes/OSPF/General form to view and change the dynamic routing settings for OSPF (see Network/Routes/OSPF/General form).

Figure 34 Network/Routes/OSPF/General form



History: Network->Routes->OSPF->General

Oct 4, 2005 8:20:27 AM

OSPF Dynamic Route Settings

Status:	disabled	
Spf Interval:	5	(0 - 65535)
Spf Hold Time:	10	(0 - 65535)
Router Id 1:	0.0.0.0	(format: 10.10.1.75)
Router Id 2:	0.0.0.0	(format: 10.10.1.76)

Fields and buttons on the Network/Route/OSPF/General form are as follows:

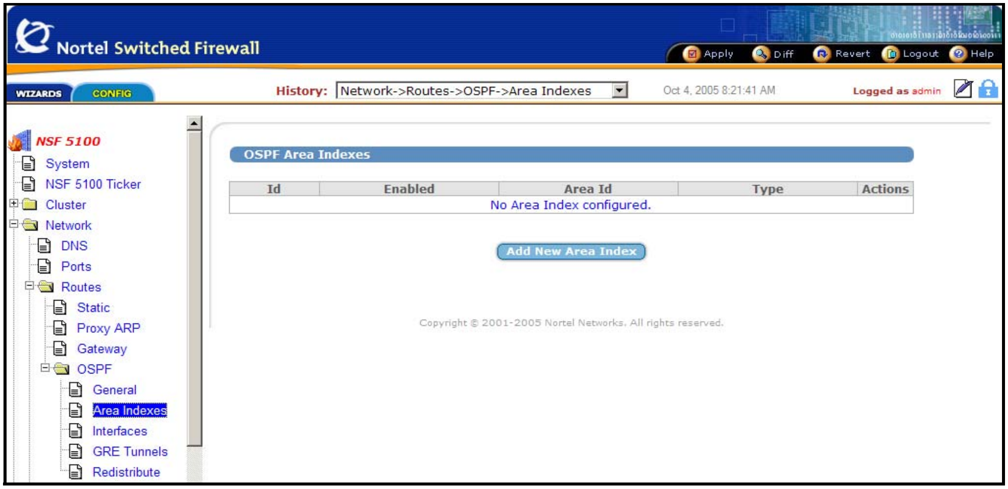
- Status displays a list with the following selections:
  - □ Disabled disables OSPF.
  - □ Enabled enables OSPF.
- Spf Interval provides an entry field to set the time interval, in seconds, between each calculation of the Shortest Path First (SPF).
- Spf Hold Time provides an entry field to set the minimum time OSPF retains a shortest-path calculation result to prevent another calculation from occurring too soon.

- Router Id 1 provides an entry field to set the OSPF Router ID for the first Firewall host. **TIP**: OSPF uses the router ID to identify the routing device. If no router ID is specified, or if the router ID is set to 0.0.0.0, the Firewall host is automatically selected as the router ID.
- Router Id 2 provides an entry field to set the OSPF Router ID for the second Firewall host.
- Save Setting submits the changes to the pending configuration.

Network/Routes/OSPF/Area Indexes form

Use the Network/Routes/OSPF/Area Indexes form to view and change the OSPF Area Index settings (see Network/Routes/OSPF/Area Indexes form).

Figure 35 Network/Routes/OSPF/Area Indexes form



History: Network->Routes->OSPF->Area Indexes

Oct 4, 2005 8:21:41 AM

Logged as admin

OSPF Area Indexes

Id	Enabled	Area Id	Type	Actions
No Area Index configured.				

Copyright © 2001-2005 Nortel Networks. All rights reserved.

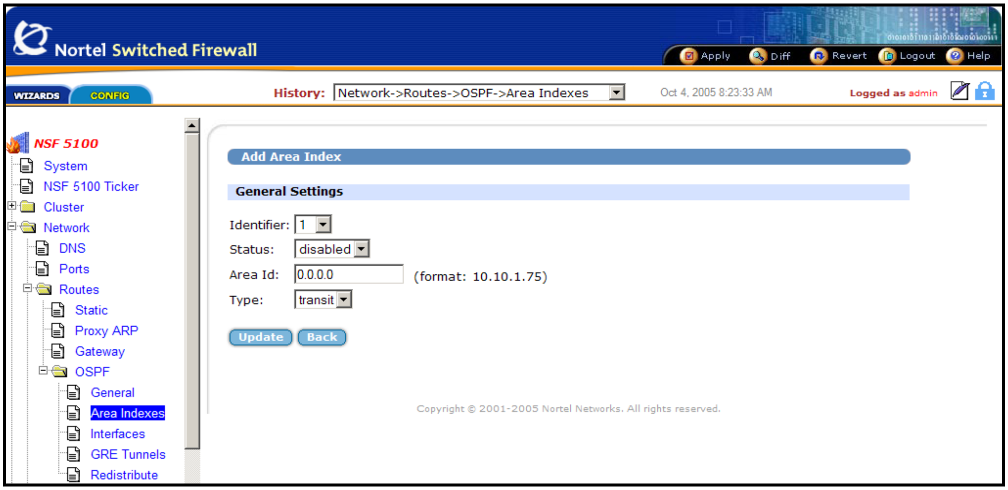
Fields and buttons on the Network/Routes/OSPF/Area Indexes form are as follows:

- Id provides the index number for the Area Index attached to the Firewall.
- Enabled indicates whether the Area Index is enabled or disabled.
- Area Id provides the IP address identifying the Area Index.
- Type indicates whether the Area Index is Transit (default) or Stub.
- Actions provides the following selections if an Area ID is present:
  - Delete deletes the Area Index adjacent to the button.
  - Modify opens a form for modifying the Area Index adjacent to the button.
- Add New Area Index opens a form for configuring a new Area Index (see Network/Routes/OSPF/Area Indexes Add Area Index form on page 61).

Network/Routes/OSPF/Area Indexes Add New form

Use the Network/Routes/OSPF/Area Indexes Add New form to configure a new Area Index.

Figure 36 Network/Routes/OSPF/Area Indexes Add Area Index form



Identifier: 1
Status: disabled
Area Id: 0.0.0.0 (format: 10.10.1.75)
Type: transit

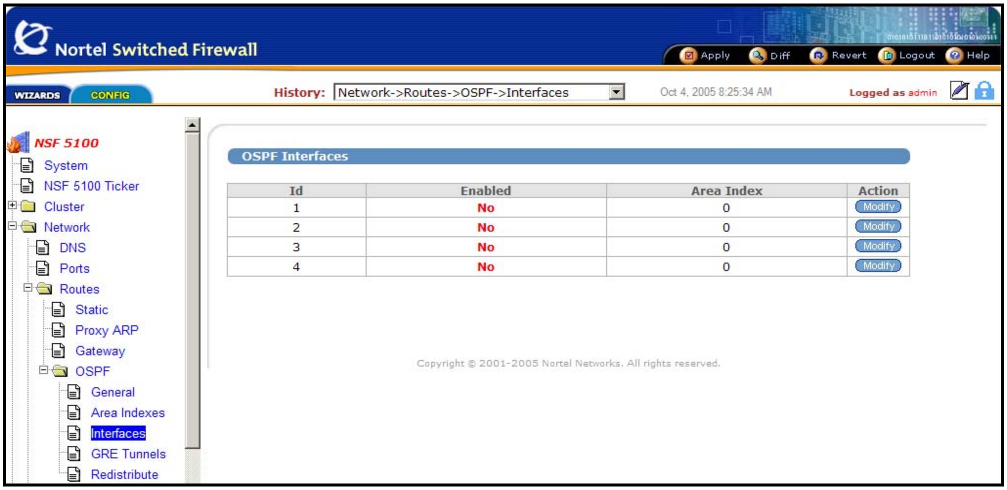
Fields and buttons on the Network/Routes/OSPF/Area Indexes Add Area Index form are as follows:

- Identifier provides a list with a numbers in a range from 1 to 16.
- Status provides a list with the following two selections:
  - Enabled enables the area.
  - Disabled disables the area.
- Area Id provides an entry field to set the OSPF area number. **TIP**: Use dotted decimal notation.
- Type provides a list with the following two selections to set the area type:
  - transit
  - stub
- Update submits the changes to the pending configuration.
- Back returns to the Network/Routes/OSPF/Area Indexes form without submitting changes to the pending configuration.

Network/Routes/OSPF/Interfaces form

Use the Network/Routes/OSPF/Interfaces form to display and change the OSPF Interfaces settings that are required to attach an IP network to an OSPF area (see Network/Routes/OSPF/Interfaces form).

Figure 37 Network/Routes/OSPF/Interfaces form



History: Network->Routes->OSPF->Interfaces

Oct 4, 2005 8:25:34 AM

Logged as admin

OSPF Interfaces

Id	Enabled	Area Index	Action
1	No	0	Modify
2	No	0	Modify
3	No	0	Modify
4	No	0	Modify

Copyright © 2001-2005 Nortel Networks. All rights reserved.

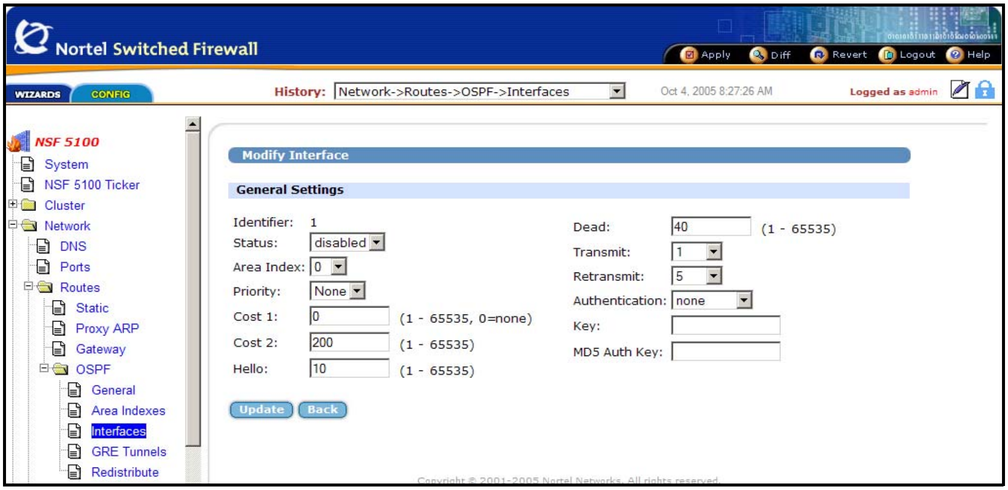
Fields and buttons on the Network/Routes/OSPF/Interfaces form are as follows:

- Id provides a numerical ID, between 1 and 255, for the interface.
- Enabled indicates OSPF Interfaces status as Yes or No.
- Area Index sets the OSPF area index to attach to the network for the current IP interface.
- Action provides a Modify button used to access a form to modify or update the OSPF Interfaces. The Modify form displays a modified interface if interfaces are present (see Network/Routes/OSPF/Interfaces Modify form on page 63).

Network/Routes/OSPF/Interfaces Modify form

Use the Network/Routes/OSPF/Interfaces Modify form to modify a selected interface.

Figure 38 Network/Routes/OSPF/Interfaces Modify form



History: Network->Routes->OSPF->Interfaces

Modify Interface

General Settings

Identifier: 1

Status: disabled

Area Index: 0

Priority: None

Cost 1: 0 (1 - 65535, 0=none)

Cost 2: 200 (1 - 65535)

Hello: 10 (1 - 65535)

Dead: 40 (1 - 65535)

Transmit: 1

Retransmit: 5

Authentication: none

Key:

MD5 Auth Key:

Fields and buttons on the Network/Routes/OSPF/Interfaces Modify form are as follows:

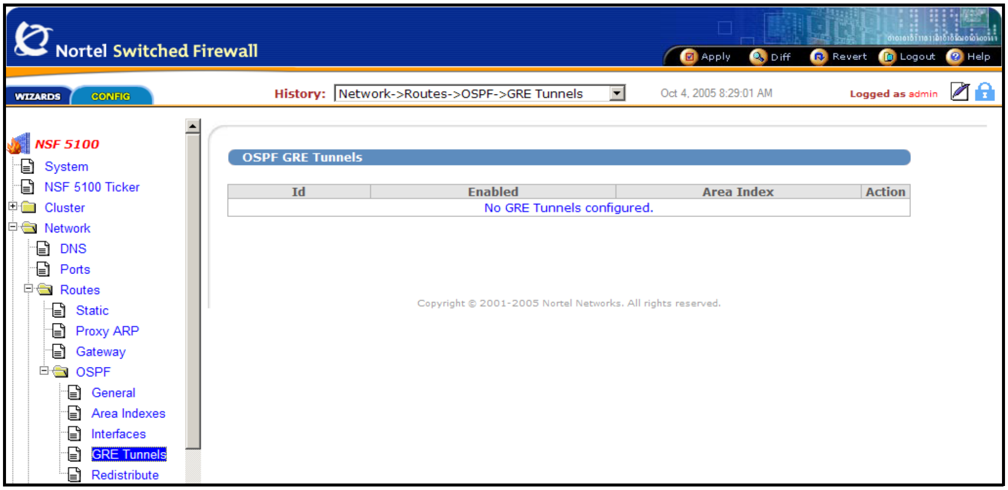
- Identifier sets the numerical ID for the interface between 1 and 255.
- Status provides a list with the following two options:
  - enabled enables the interface operational status.
  - disabled disables the interface operational status.
- Area Index provides a list to set the OSPF area index to attach to the network for this IP interface.
- Priority sets the IP interface (IF) priority used when electing a Designated Router (DR) and Backup Designated Router (BDR) for the area. **TIP**: The default is 1.
- Cost 1 provides an entry field to set the cost of output routes for first Firewall host.
- Cost 2 provides an entry field to set the cost of output routes for the second Firewall host.
- Hello provides an entry field to set the hello interval in seconds.
- Dead provides an entry field to set the router dead interval in seconds.
- Transmit provides a list to set the transmit delay in seconds.
- Retransmit provides a list to set the time interval in seconds.

- Authentication provides a list to set the authentication type for the interface, with the following selections:
  - □ None
  - □ Password
  - □ MD5
- Key provides an entry field to set the password used for OSPF authentication when the authentication options is set to *password*.
- MD5 Auth Key provides an entry field to set the password used for OSPF authentication when the authentication options is set to *MD5*.
- Update submits the changes to the pending configuration.
- Back returns to the Network/Routes/OSPF Interfaces without submitting the changes to the pending configuration.

Network/Routes/OSPF/GRE Tunnels form

Use the Network/Routes/OSPF/GRE Tunnels form to display and change the GRE tunnels (see Network/Routes/OSPF/GRE Tunnels form).

Figure 39 Network/Routes/OSPF/GRE Tunnels form



History: Network->Routes->OSPF->GRE Tunnels

Oct 4, 2005 8:29:01 AM

Logged as admin

OSPF GRE Tunnels

Id	Enabled	Area Index	Action
No GRE Tunnels configured.			

Copyright © 2001-2005 Nortel Networks. All rights reserved.

Fields and buttons on the Network/Routes/OSPF/GRE Tunnels form are as follows:

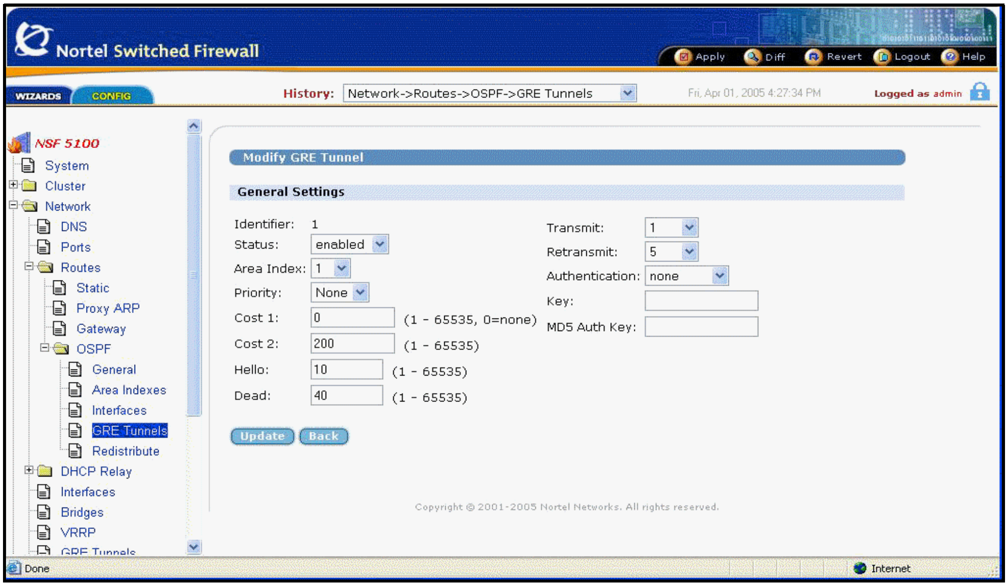
- Id provides the numerical ID for the GRE tunnel.
- Enabled provides the status of the GRE tunnel.

- Area Index sets the OSPF area index to attach to the network for the current GRE Tunnel.
- Action provides the following two options:
  - Delete deletes a selected GRE tunnel.
  - Modify provides a form to modify a selected GRE tunnel (see Network/Routes/OSPF/GRE Tunnels Modify form).

Network/Routes/OSPF/GRE Tunnels Modify form

Use the Network/Routes/OSPF/GRE Tunnels Modify form to modify GRE tunnel settings.

Figure 40 Network/Routes/OSPF/GRE Tunnels Modify form



History: Network->Routes->OSPF->GRE Tunnels

Fri, Apr 01, 2005 4:27:34 PM

Logged as admin

Identifier: 1

Status: enabled

Area Index: 1

Priority: None

Cost 1: 0 (1 - 65535, 0=none)

Cost 2: 200 (1 - 65535)

Hello: 10 (1 - 65535)

Dead: 40 (1 - 65535)

Transmit: 1

Retransmit: 5

Authentication: none

Key:

MD5 Auth Key:

Fields and buttons on the Network/Routes/OSPF/GRE Tunnels Modify form are as follows:

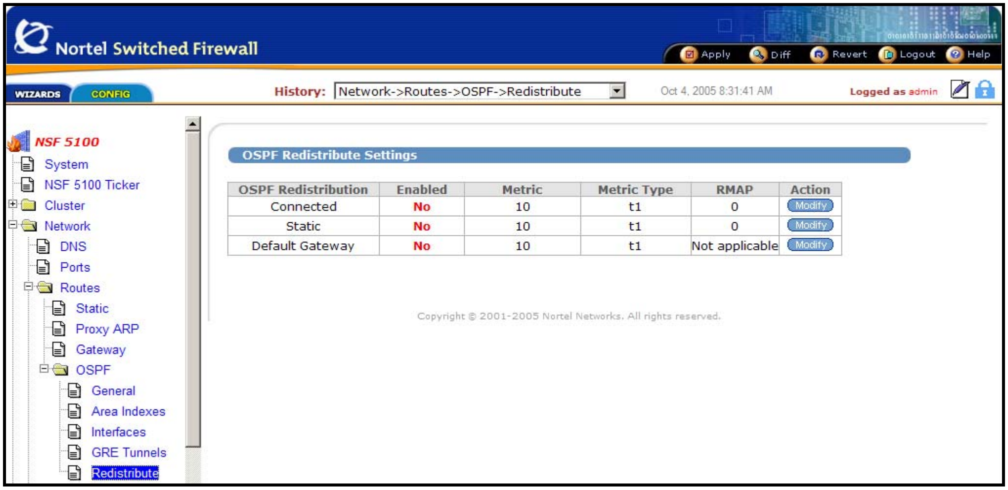
- Identifier provides the numerical ID of the GRE tunnel.
- Status provides a list with the following two choices:
  - Enabled enables the GRE tunnel.
  - Disabled disables the GRE tunnel.
- Area Index provides a list to select a value to set the OSPF area index to attach to the network for the current GRE Tunnel.

- Priority provides a list to set the GRE Tunnel priority used to elect a Designated Router (DR) and Backup Designated Router (BDR) for the area. **TIP**: A value of 0 specifies that the elected GRE Tunnel is DROTHER and cannot be used as a DR or BDR.
- Cost1 provides an entry field to set the cost of output routes for the first Firewall host. **TIP**: Cost is based on bandwidth. Low cost indicates high bandwidth.
- Cost 2 provides an entry field to sets the cost of output routes for the second Firewall host.
- Hello provides an entry field to set the hello interval in seconds. **TIP**: The value must be the same on all routing devices within the area.
- Dead provides an entry field to set the router dead interval value, in seconds. **TIP**: The dead value is typically four times the value of "hello." This value must be the same on all routing devices within the same area.
- Transmit provides a list to set the transmit delay, in seconds. **TIP**: This value must be the same on all routing devices within the area.
- Retransmit provides a list to set the time interval, in seconds, between each transmission of LSAs to adjacencies on this GRE Tunnel. **TIP**: This value must be the same on all routing devices within the area.
- Authentication provides a list to set the authentication type.
- Key provides an entry field to specify the password to be used for OSPF authentication. **TIP**: Specify a type 1 (plain text) password of up to 16 characters.
- MD5 Auth Key provides an entry field to set the password to be used for OSPF authentication. **TIP**: Specify a password of up to 16 characters.
- Update submits the OSPF GRE changes to the pending configuration and returns to the Network/Routes/OSPF/GRE form.
- Back returns to the Network/Routes/OSPF/GRE Tunnels page without submitting the OSPF GRE settings to the pending configuration.

Network/Routes/OSPF/Redistribute form

Use the Network/Routes/OSPF/Redistribute form to display and modify the OSPF Redistribution settings (see Network/Routes/OSPF/Redistribute form).

Figure 41 Network/Routes/OSPF/Redistribute form



History: Network->Routes->OSPF->Redistribute

Oct 4, 2005 8:31:41 AM

Logged as admin

OSPF Redistribute Settings

OSPF Redistribution	Enabled	Metric	Metric Type	RMAP	Action
Connected	No	10	t1	0	Modify
Static	No	10	t1	0	Modify
Default Gateway	No	10	t1	Not applicable	Modify

Copyright © 2001-2005 Nortel Networks. All rights reserved.

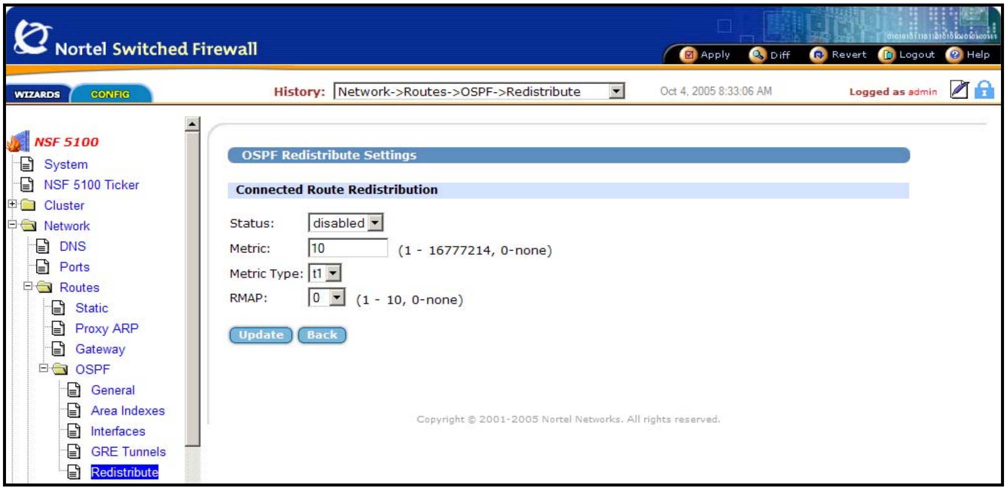
Fields and buttons on the Network/Routes OSPF/Redistribute form are as follows:

- OSPF Redistribution displays the following three settings:
  - Connected
  - Static
  - Default Gateway
- Enabled
  - Yes indicates that the setting is enabled.
  - No indicates that the setting is disabled.
- Metric is the numeric value used by OSPF for all redistributed routes.
- Metric Type is the OSPF exterior metric type for redistributed routes.
- RMAP is the OSPF Connected Redistribute RMAP number.
- Action provides the following selection:
  - Modify provides a form to modify the connected route redistribution (see Network/Routes/OSPF/Redistribute Modify form on page 68).

Network/Routes/OSPF/Redistribute Modify form

Use the Network/Routes/OSPF/Redistribute Modify form to modify the connected route redistribution.

Figure 42 Network/Routes/OSPF/Redistribute Modify form



History: Network->Routes->OSPF->Redistribute

Oct 4, 2005 8:33:06 AM

Logged as admin

OSPF Redistribute Settings

Connected Route Redistribution

Status:	disabled
Metric:	10 (1 - 16777214, 0-none)
Metric Type:	t1
RMAP:	0 (1 - 10, 0-none)

Copyright © 2001-2005 Nortel Networks. All rights reserved.

Fields and buttons on the Network/Routes/OSPF/Redistribute Modify form are as follows:

- Status provides a list with two selections:
  - enabled enables the connected route redistribution
  - disabled disables the connected route redistribution
- Metric provides an entry field for the metric used by all redistributed connected routes.
- Metric Type provides a list with the following two selections of OSPF exterior metric types for redistributed routes:
  - t1 applies additional calculations
  - t2 does not apply additional calculations
- RMAP provides a list to select values in a range from 0 to 10.
- Update submits the changes to the pending configuration.
- Back returns to the Network/Routes/OSPF/Redistribute form without submitting the changes to the pending configuration.

DHCP Relay forms

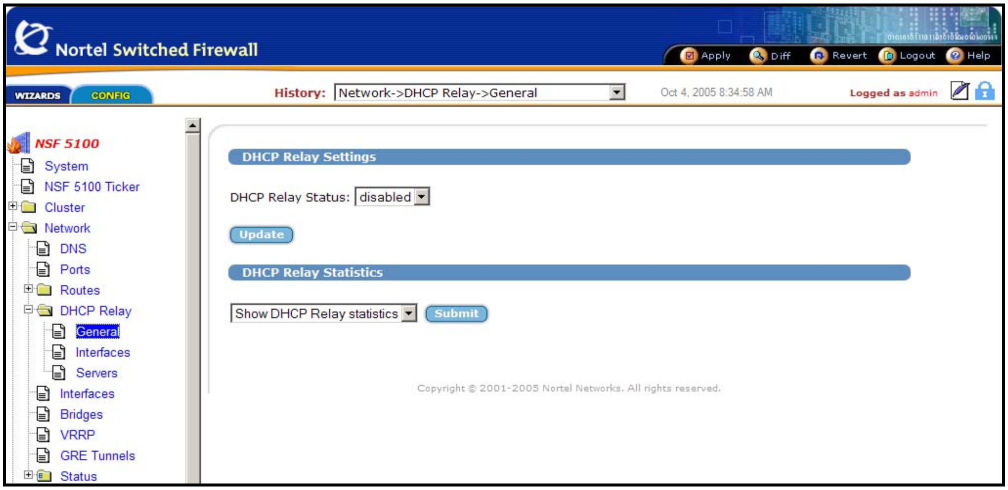
The three DHCP Relay forms are:

- General
- Interfaces
- Servers

Network/DHCP Relay/General form

Use the Network/DHCP Relay/General form to display DHCP Relay settings and statistics (see Network/DHCP Relay/General form).

Figure 43 Network/DHCP Relay/General form



History: Network->DHCP Relay->General

Oct 4, 2005 8:34:58 AM

Logged as admin

DHCP Relay Settings

DHCP Relay Status: disabled

DHCP Relay Statistics

Show DHCP Relay statistics

Copyright © 2001-2005 Nortel Networks. All rights reserved.

The Network/DHCP Relay/General form is presented in the following two sections:

- DHCP Relay Settings
- DHCP Relay Statistics

Fields and buttons on the form are as follows:

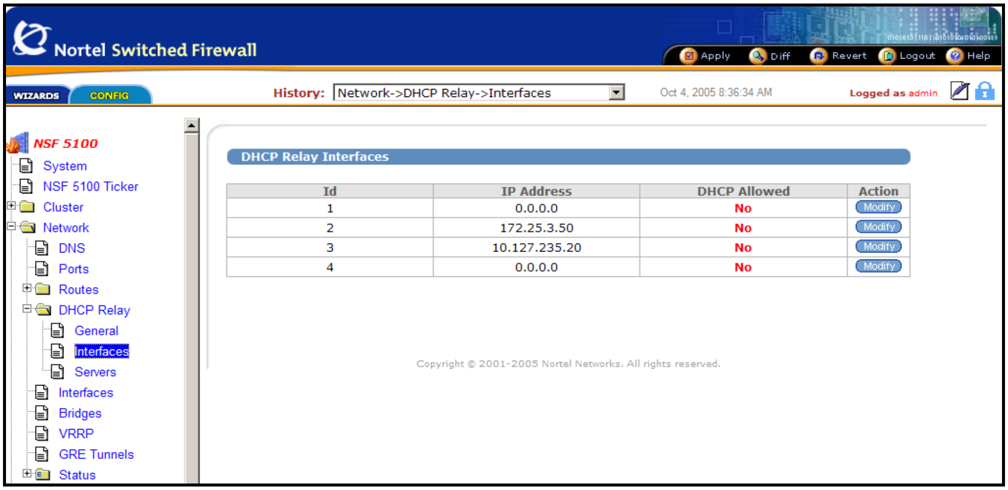
- DHCP Relay Settings
  - DHCP Relay Status provides a list with the following two selections:
    - Disabled disables DHCP Relay.
    - Enabled enables DHCP Relay.
  - Update submits changes to the pending configuration.

- DHCP Relay Statistics
  - DHCP Relay Statistics provides a list containing the following two selections:
    - Show DHCP Relay statistics
    - Clear DHCP Relay statistics
  - Submit submits changes to the pending configuration.

Network/DHCP Relay/Interfaces form

Use the Network/DHCP Relay/Interfaces form to configure the DHCP relay requests into the network (see Network/DHCP Relay/Interfaces form).

Figure 44 Network/DHCP Relay/Interfaces form



History: Network->DHCP Relay->Interfaces

DHCP Relay Interfaces

Id	IP Address	DHCP Allowed	Action
1	0.0.0.0	No	Modify
2	172.25.3.50	No	Modify
3	10.127.235.20	No	Modify
4	0.0.0.0	No	Modify

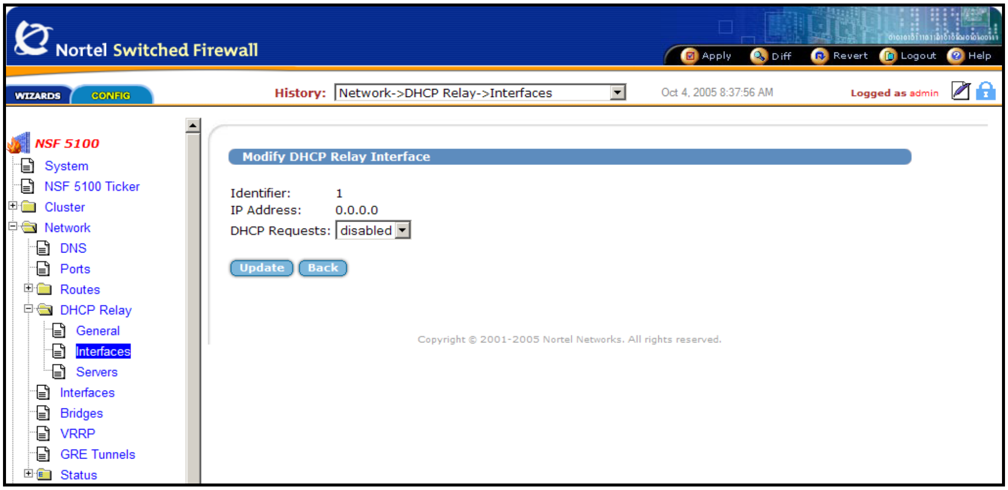
Fields and buttons on the network/DHCP Relay/Interfaces form are as follows:

- Id provides the interface identifier.
- IP Address is the interface IP address.
- DHCP Allowed
  - Yes
  - No
- Action provides the following option:
  - Modify is used to change the selected DHCP Relay Interface (see Network/DHCP Relay/Interfaces Modify form on page 71).

Network/DHCP Relay/Interfaces Modify form

Use the Network/DHCP Relay/Interfaces Modify form to modify a selected DHCP Relay Interface.

Figure 45 Network/DHCP Relay/Interfaces Modify form



Modify DHCP Relay Interface

Identifier: 1
IP Address: 0.0.0.0
DHCP Requests: disabled

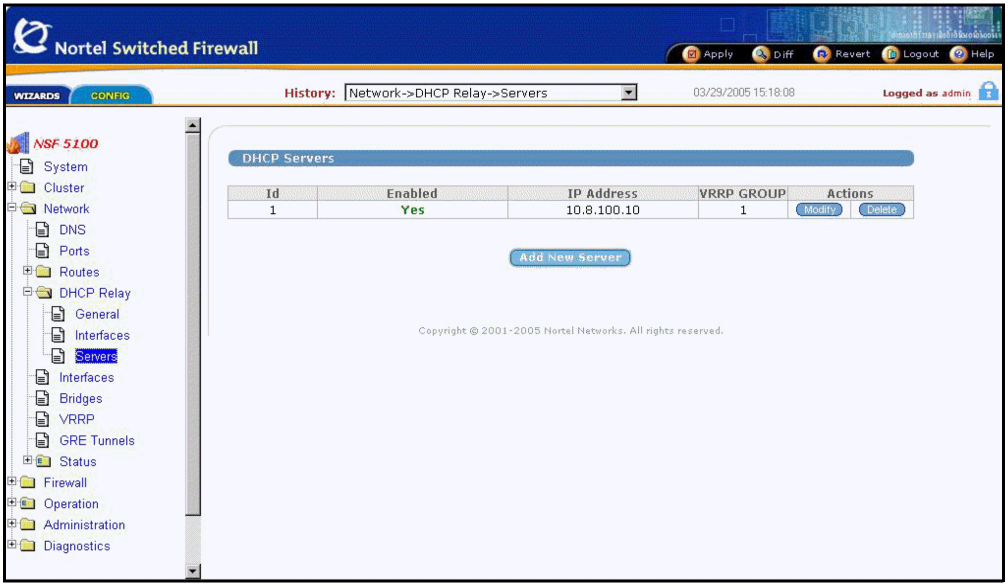
Fields and buttons on the Network/DHCP Relay/Interfaces Modify form are as follows:

- Identifier is the interface identifier.
- IP Address is the interface IP address.
- DHCP Requests enables or disables access for DHCP clients through the interface.
- Update submits the changes to the pending configuration.
- Back returns to the Network/DHCP/Relay/Interfaces form without submitting changes to the pending configuration.

Network/DHCP Relay/Servers form

Use the Network/DHCP Relay/Servers form to display and modify the information about the DHCP Relay Servers (see Network/DHCP Relay/Servers form).

Figure 46 Network/DHCP Relay/Servers form



History: Network->DHCP Relay->Servers

03/29/2005 15:18:08

Logged as admin

DHCP Servers

Id	Enabled	IP Address	VRRP GROUP	Actions	
1	Yes	10.8.100.10	1	Modify	Delete

Copyright © 2001-2005 Nortel Networks. All rights reserved.

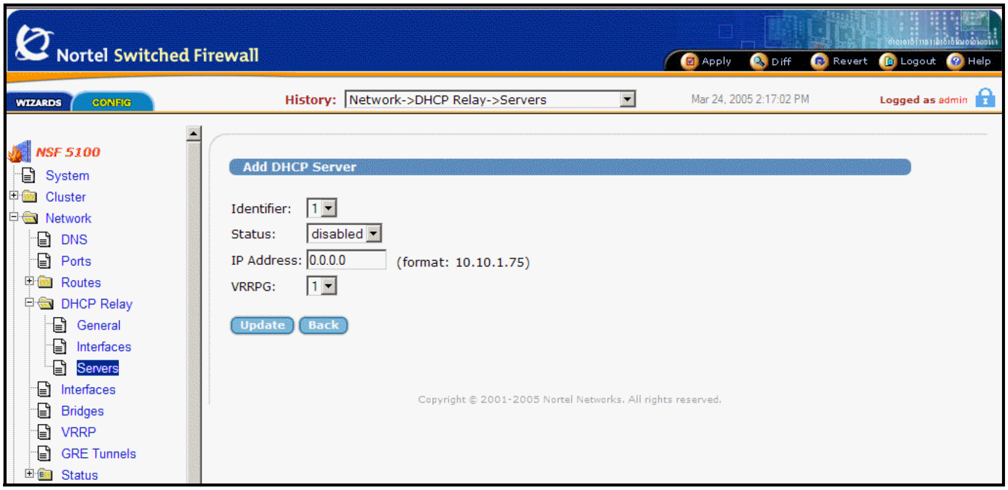
Fields and buttons on the Network/DHCP Relay/Servers form, when DHCP servers are configured, are as follows:

- Id provides the internal ID of the DHCP server.
- Enabled
  - Yes indicates that the DHCP server is enabled.
  - No indicates that the DHCP server is disabled.
- IP Address specifies the IP address of the DHCP server.
- VRRP Group specifies the affinity to VRRP Group in active-active mode.
- Actions provides the following two options:
  - Modify provides a form to modify the server information.
  - Delete deletes the selected server.
- Add New Server (see Network/DHCP Relay/Servers Add New Server form on page 73).

Network/DHCP Relay/Servers Add New Server form

Use the Network/DHCP Relay/Servers Add New Server form to add a new DHCP server.

Figure 47 Network/DHCP Relay/Servers Add New Server form



History: Network->DHCP Relay->Servers

Mar 24, 2005 2:17:02 PM

Logged as admin

Add DHCP Server

Identifier: 1

Status: disabled

IP Address: 0.0.0.0 (format: 10.10.1.75)

VRRPG: 1

Copyright © 2001-2005 Nortel Networks. All rights reserved.

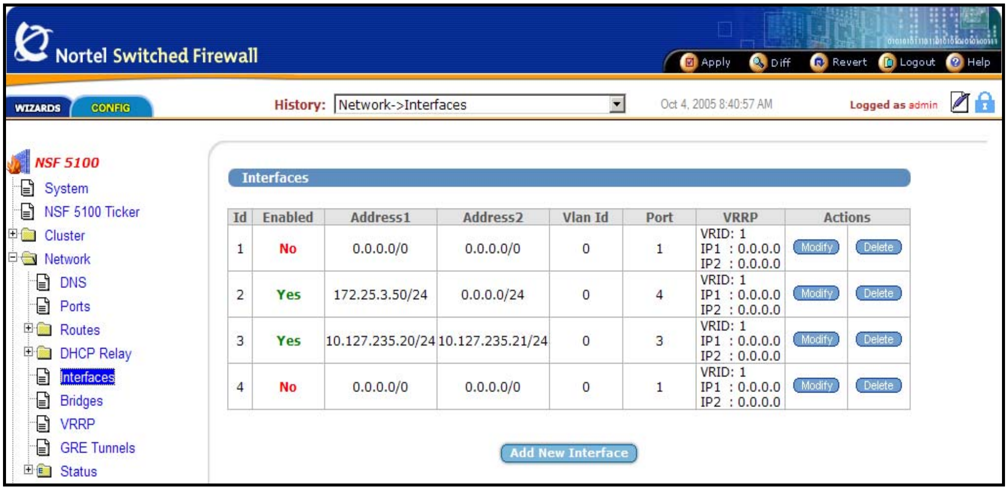
Fields and buttons on the Network/DHCP Relay/Servers Add New Server form are as follows:

- Identifier provides a numerical list with a range from 1 to 8 to specify the internal ID of the DHCP server.
- Status provides a list with the following two selections:
  - Enabled enables the user of DHCP services.
  - Disabled disables the user of DHCP services.
- IP Address provides a field to specify the IP address of the DHCP server.
- VRRPG provides a numerical list with a choice of 1 or 2 to specify the affinity to VRRP Group in active-active mode.
- Update submits the changes to the pending configuration.
- Back returns to the Network/DHCP Relay Servers form without submitting changes to the pending configuration.

Interfaces form

Use the Network/Interfaces form to view and configure the settings for individual interfaces (see Network/Interfaces form).

Figure 48 Network/Interfaces form



History: Network->Interfaces

Oct 4, 2005 8:40:57 AM

Logged as admin

Interfaces

Id	Enabled	Address1	Address2	Vlan Id	Port	VRRP	Actions	
1	No	0.0.0.0/0	0.0.0.0/0	0	1	VRID: 1 IP1 : 0.0.0.0 IP2 : 0.0.0.0	Modify	Delete
2	Yes	172.25.3.50/24	0.0.0.0/24	0	4	VRID: 1 IP1 : 0.0.0.0 IP2 : 0.0.0.0	Modify	Delete
3	Yes	10.127.235.20/24	10.127.235.21/24	0	3	VRID: 1 IP1 : 0.0.0.0 IP2 : 0.0.0.0	Modify	Delete
4	No	0.0.0.0/0	0.0.0.0/0	0	1	VRID: 1 IP1 : 0.0.0.0 IP2 : 0.0.0.0	Modify	Delete

The Firewall can be configured with up to 255 IP interfaces, each representing the Firewall on the IP subnet. Fields and buttons on the Network/Interfaces form are as follows:

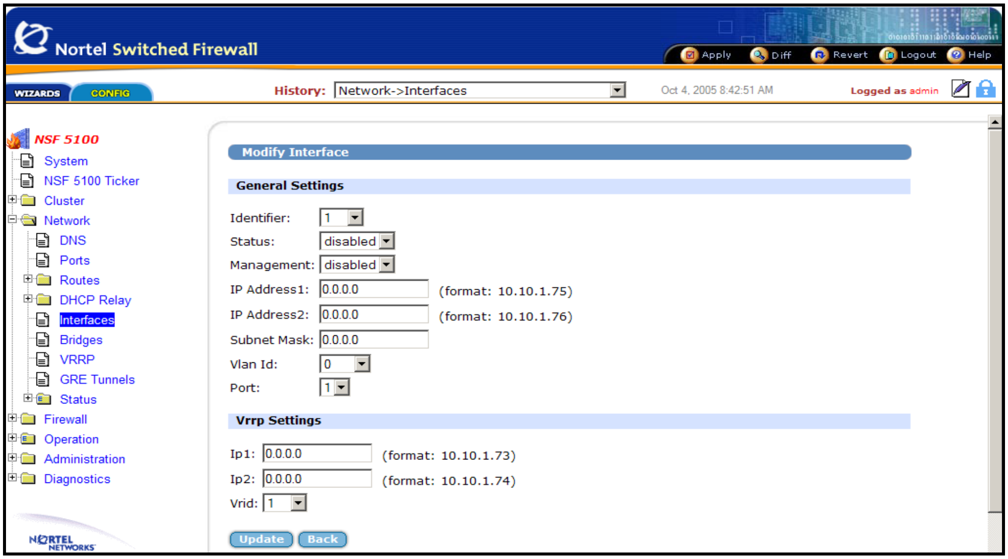
- Id specifies the numerical ID, between 1 and 255, for the interface and can be used to specify the interface when configuring a new route.
- Enabled
  - Yes indicates that the interface is enabled.
  - No indicates that the interface is disabled.
- Address1 specifies the IP address of the interface. **TIP**: Use the dotted decimal notation.
- Address2 specifies the second IP address of the interface. **TIP**: Address2 is used in an active-active and active-standby VRRP configuration.
- Vlan Id specifies the numerical ID for a VLAN on the interface.
- Port associates the interface with a single port.
- VRRP specifies the Virtual Router ID and IP address of IP interfaces configured for high-availability and active-active. **TIP**: Use the virtual IP address to access the firewall with enhanced security.
- Actions provides the following two options:

  - Modify (only visible if interfaces are present) is used to modify a displayed interface (see Network/Interfaces Modify form on page 75).
  - Delete (only visible if interfaces are present) is used to delete an interface from the system.
- Add New Interface adds a new interface to the configuration (see Network/Interfaces Add New Interface form on page 77).

Network/Interfaces Modify form

Use the Network/Interfaces Modify form to modify interfaces.

Figure 49 Network/Interfaces Modify form



Modify Interface

General Settings

Identifier: 1
Status: disabled
Management: disabled
IP Address1: 0.0.0.0 (format: 10.10.1.75)
IP Address2: 0.0.0.0 (format: 10.10.1.76)
Subnet Mask: 0.0.0.0
Vlan Id: 0
Port: 1

Vrrp Settings

Ip1: 0.0.0.0 (format: 10.10.1.73)
Ip2: 0.0.0.0 (format: 10.10.1.74)
Vrid: 1

Fields and buttons on the Network/Interfaces Modify form are as follows:

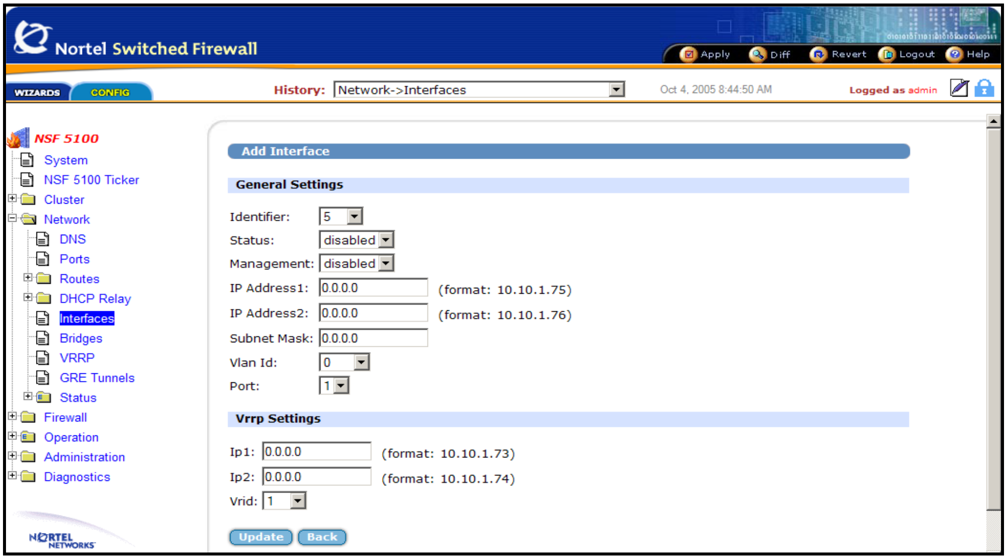
- General Settings
  - Identifier provides a list to select a numerical ID, between 1 and 255, for the interface.
  - Status provides a list to enable or disable the interface operation.
  - Management provides a list to enable or disable management through the interface.
  - IP Address 1 provides an entry field to specify the IP address for the interface of the Firewall host 1.
  - IP Address 2 provides an entry field to specify the IP address for the interface of the Firewall host 2.

  - Subnet Mask provides an entry field to specify the subnet mask of the interface.
  - Vlan Id provides a list to select the numerical ID, between 0 and 4094, for the VLAN.
  - Port provides a list to select a port number, between 1 and 6 for the 5109 and 5111-NE1 hardware platforms, or 1 and 4 for other hardware platforms, to associate with the interface ID number.
- VRRP Settings
  - Ip1 provides an entry field to specify the first virtual IP address for the interface.
  - Ip2 provides an entry field to specify the second virtual IP address for the interface (applied for VRRP Active-Active).
  - Vrid provides a list to select a numerical ID, between 1 and 255, for the virtual router.
- Update submits changes to the pending configuration.
- Back returns to the Network/Interfaces form without submitting changes to the pending configuration.

Network/Interfaces Add Interface form

Use the Network/Interfaces Add Interface form to add a new interface.

Figure 50 Network/Interfaces Add New Interface form



History: Network->Interfaces

Oct 4, 2005 8:44:50 AM

Logged as admin

Add Interface

General Settings

Identifier: 5

Status: disabled

Management: disabled

IP Address1: 0.0.0.0 (format: 10.10.1.75)

IP Address2: 0.0.0.0 (format: 10.10.1.76)

Subnet Mask: 0.0.0.0

Vlan Id: 0

Port: 1

Vrrp Settings

Ip1: 0.0.0.0 (format: 10.10.1.73)

Ip2: 0.0.0.0 (format: 10.10.1.74)

Vrid: 1

Fields and buttons on the Network/Interfaces Add New Interface form are as follows:

- General Settings
  - Identifier provides a list to select a numerical ID, between 1 and 255, for the interface.
  - Status provides a list to enable or disable the interface operation.
  - Management provides a list to enable of disable management through the interface.
  - IP Address 1 provides an entry field to specify the IP address for the interface of the Firewall host 1.
  - IP Address 2 provides an entry field to specify the IP address for the interface of the Firewall host 2.
  - Subnet Mask provides an entry field to specify the subnet mask of the interface.
  - Vlan Id provides a list to select the numerical ID, between 0 and 4094, for the VLAN.
  - Port provides a list to select a port number to associate with the interface ID number.
- VRRP Settings
  - Ip1 provides an entry field to specify the first virtual IP address of the interface.

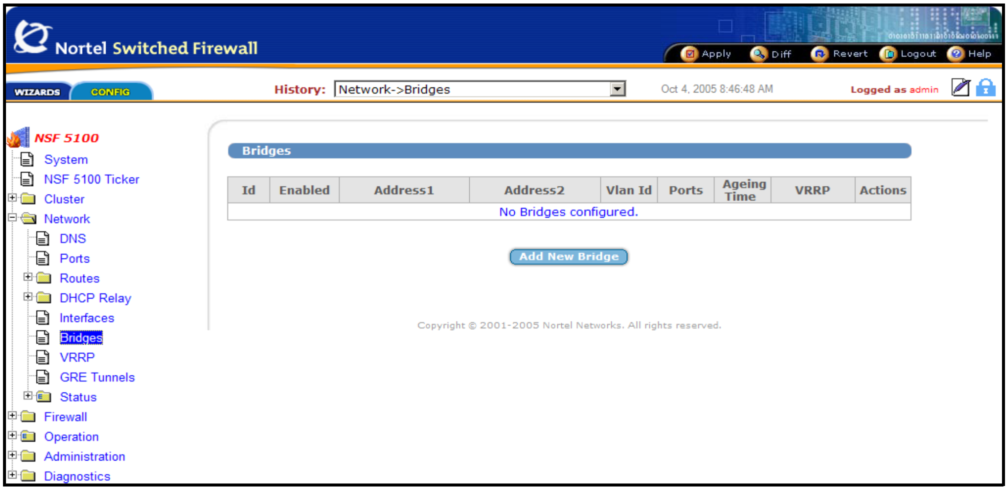
- □ Ip2 provides an entry field to specify the second virtual IP address for the interface (applied for VRRP Active-Active).
- □ Vrid provides a list to select a numerical ID, between 1 and 255, for the virtual router.

- Update submits the changes to the pending configuration.
- Back returns to the Network/Interfaces form without submitting changes to the pending configuration.

Bridges form

Use the Network Bridges form to view and configure settings for bridges (see Network/Bridges form).

Figure 51 Network/Bridges form



History: Network->Bridges

Oct 4, 2005 8:46:48 AM

Logged as admin

Bridges

Id	Enabled	Address1	Address2	Vlan Id	Ports	Ageing Time	VRRP	Actions

No Bridges configured.

Copyright © 2001-2005 Nortel Networks. All rights reserved.

Fields and buttons on the Network/Bridges form are as follows:

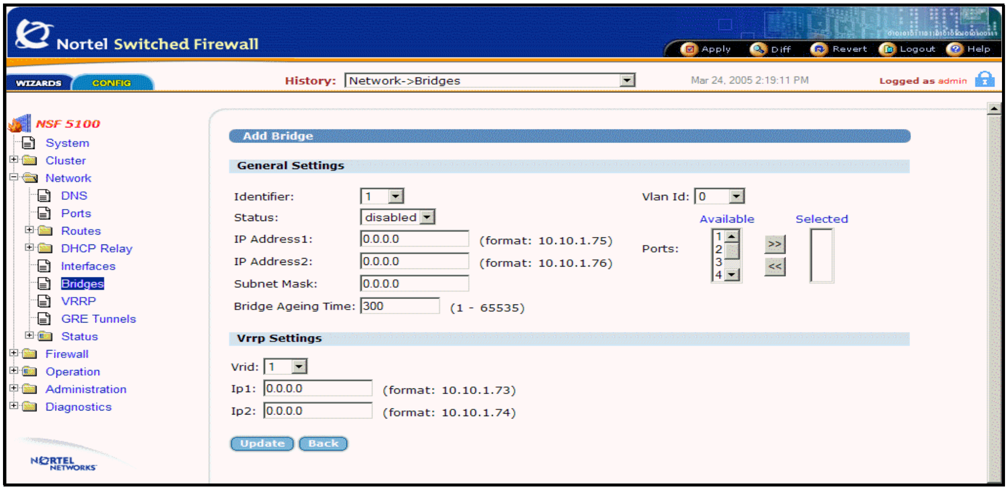
- Id specifies the numerical ID, between 1 and 25, for the bridge.
- Enabled displays the bridge operational status as Yes or No.
- Address1 specifies the address #1 of the bridge.
- Address2 specifies the address #2 of the bridge.
- Vlan Id specifies the numerical ID, between 0 and 4094, for the VLAN.
- Ports specifies the port number associated with the bridge ID.
- Ageing Time specifies the bridge ageing time in seconds.

- VRRP specifies the virtual router ID and IP address of the IP interface configured for high availability or active–active.
- Actions provides the following two options:
  - □ Delete deletes the selected bridge.
  - □ Modify provides a form to modify the selected bridge.
- Add New Bridge (see Network/Bridges Add New Bridge form on page 79).

Network/Bridges Add New Bridge form

Use the Network/Bridges Add New Bridge form to add a new bridge to the configuration.

Figure 52 Network/Bridges Add New Bridge form



History: Network->Bridges

Mar 24, 2005 2:19:11 PM

Logged as admin

Add Bridge

General Settings

Identifier: 1

Status: disabled

IP Address1: 0.0.0.0 (format: 10.10.1.75)

IP Address2: 0.0.0.0 (format: 10.10.1.76)

Subnet Mask: 0.0.0.0

Bridge Ageing Time: 300 (1 - 65535)

Vlan Id: 0

Ports: Available 1 2 3 4 Selected

Vrrp Settings

Vrid: 1

Ip1: 0.0.0.0 (format: 10.10.1.73)

Ip2: 0.0.0.0 (format: 10.10.1.74)

Fields and buttons on the Network/Bridges Add New Bridge form are as follows:

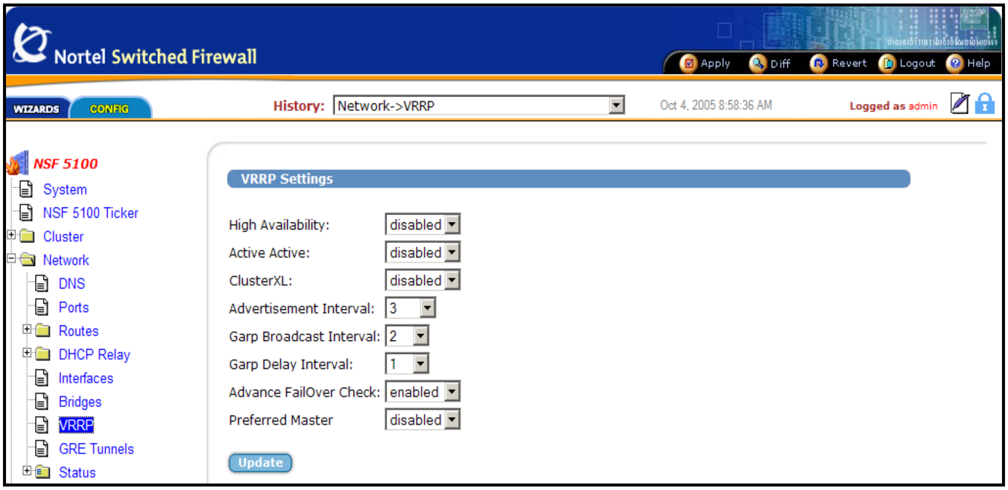
- General Settings
  - □ Identifier provides a list to select a numerical ID, between 1 and 25, for the bridge.
  - □ Status provides a list to select enabled or disabled for bridge status.
  - □ IP Address1 provides an entry field to specify real IP address #1 for the bridge.
  - □ IP Address2 provides an entry field to specify real IP address #2 for the bridge.
  - □ Subnet Mask provides an entry field to specify the subnet mast for the bridge.
  - □ Bridge Ageing Time provides an entry field to specify the bridge ageing time in seconds.
    - □ Vlan Id specifies the numerical ID, between 0 and 4094, for the VLAN.

  - Ports specifies the port number associated with the bridge ID.
- VRRP Settings
  - Vrid provides a list to select the numerical ID, between 1 and 255, for the virtual router on the bridge.
  - Ip1 provides an entry field to specify virtual IP address #1 for the interface.
  - Ip2 provides an entry field to specify virtual IP address #2 for the interface (applied for VRRP Active-Active).
  - Update submits the changes to the pending configuration.
  - Back returns to the Network/Bridges form without submitting changes to the pending configuration.

VRRP form

Use the Network/VRRP form to view and configure the VRRP parameters for the cluster (see Network/VRRP form).

Figure 53 Network/VRRP form



VRRP Settings

High Availability:	disabled
Active Active:	disabled
ClusterXL:	disabled
Advertisement Interval:	3
Garp Broadcast Interval:	2
Garp Delay Interval:	1
Advance FailOver Check:	enabled
Preferred Master	disabled

Fields and buttons on the Network/VRRP form are as follows:

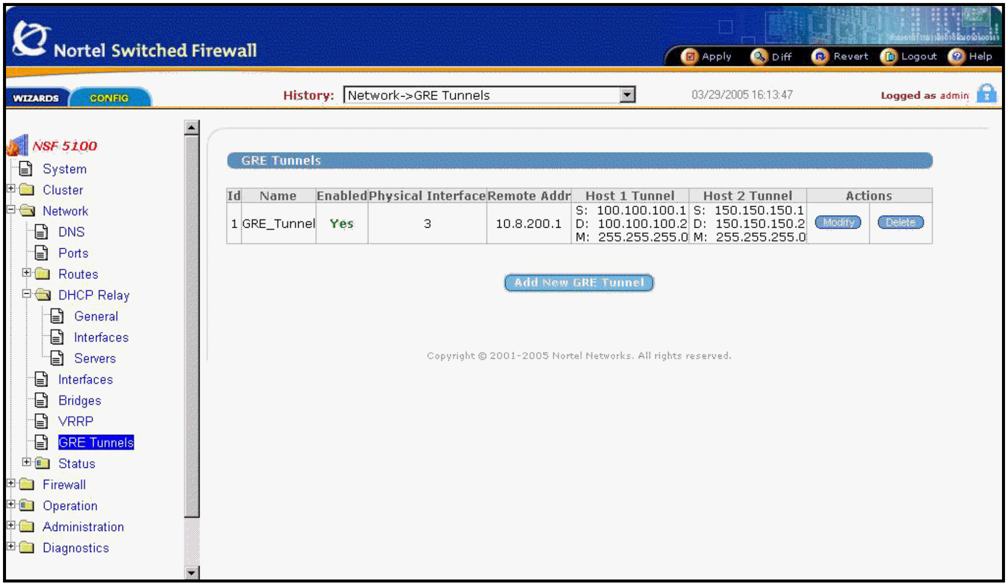
- High Availability (also called active-standby) provides a list with the following two selections:
  - Disabled indicates that high availability VRRP is disabled.

  - □ Enabled indicates that high availability VRRP is enabled. **TIP**: Two Firewall hosts must be in the cluster to apply high availability VRRP. High availability VRRP cannot be enabled when active-active VRRP or ClusterXL is enabled.
- Active-Active provides a list with the following two selections:
  - □ Disabled indicates that active-active VRRP is disabled.
  - □ Enabled indicates that active-active VRRP is enabled. **TIP**: Two Firewall hosts must be in the cluster to apply active-active VRRP. Active-active VRRP cannot be enabled when high availability VRRP or ClusterXL is enabled.
- ClusterXL provides a list with the following two selections:
  - □ Enabled indicates that ClusterXL is enabled. **TIP**: Two Firewall hosts must be in the cluster in order to apply ClusterXL. ClusterXL cannot be enabled when high availability VRRP or active–active is enabled.
  - □ Disabled indicates that ClusterXL is disabled.
- Advertisement Interval is used to set the interval between advertisement messages. **TIP**: Set the advertisement interval in seconds between 3 and 3600.
- Garp Broadcast Interval is used to set the value that, when multiplied by the Advertisement Interval, determines the interval between Gratuitous ARP (GARP) messages. TIP: The interval between GARP messages is set, in seconds, between 2 and 100.
- Garp Delay Interval displays, and permits setting of, the current GARP Delay Interval in seconds. **TIP**: The default value is 1 and the range is between 1 and 600, in seconds.
- Advance FailOver Check
  - □ Enabled indicates that AFC is enabled and the system is set to ARP before initiating a failover caused by missed VRRP advertisements.
  - □ Disabled indicates that AFC is disabled.
- Preferred Master provides a list with the following three selections:
  - □ disabled
  - □ host 1
  - □ host 2
- Update submits the changes to the pending configuration.

GRE Tunnels form

Use the Network/GRE Tunnels form to view and modify GRE Tunnels settings (see Network/GRE Tunnels form).

Figure 54 Network/GRE Tunnels form



GRE Tunnels

Id	Name	Enabled	Physical Interface	Remote Addr	Host 1 Tunnel	Host 2 Tunnel	Actions	
1	GRE_Tunnel	Yes	3	10.8.200.1	S: 100.100.100.1 D: 100.100.100.2 M: 255.255.255.0	S: 150.150.150.1 D: 150.150.150.2 M: 255.255.255.0	Modify	Delete

Fields and buttons on the Network/GRE Tunnels form are as follows:

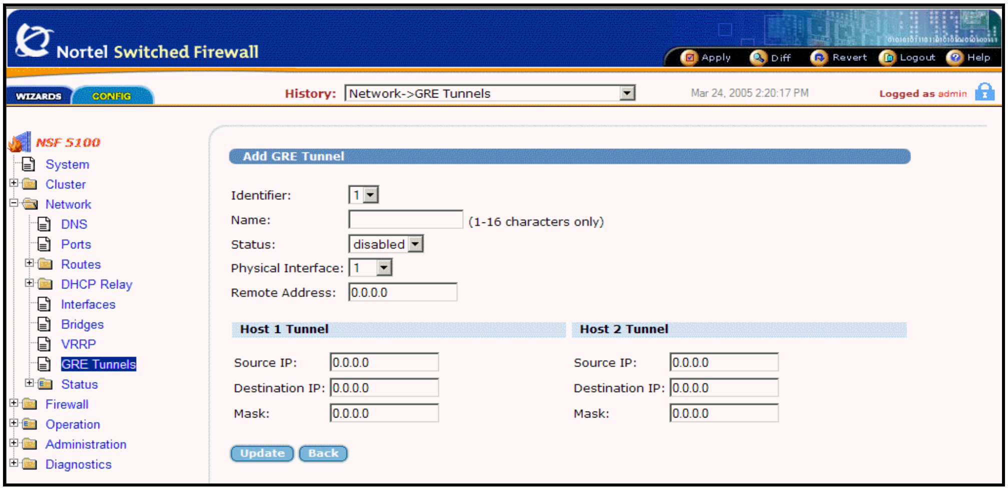
- Id specifies the numerical ID for the GRE tunnel in a range between 1 and 5.
- Name specifies the name given to the GRE tunnel.
- Enabled provides the status of the GRE tunnel.
- Physical Interface specifies the physical interface number for the GRE tunnel in a range between 1 and 255.
- Remote Addr specifies the remote IP address for the GRE tunnel.
- Host 1 Tunnel provides the tunnel source IP address, destination IP address, and IP Mask specified for host 1.
- Host 2 Tunnel provides the tunnel source IP address, destination IP address, and IP Mask specified for host 2. **TIP**: Configure host 2 when VRRP HA or Active-Active is activated.

- Actions provides the following two options:
  - □ Delete deletes the selected GRE tunnel.
  - □ Modify provides a form to modify the settings for the selected GRE tunnel.
- Add New GRE Tunnel (see Network/GRE Tunnels Add New GRE Tunnel form).

Network/GRE Tunnels Add new GRE Tunnel form

Use the Network/GRE Tunnels Add New GRE Tunnel form to add a new GRE tunnel to the configuration.

Figure 55 Network/GRE Tunnels Add New GRE Tunnel form



Add GRE Tunnel

Identifier: 1
Name: (1-16 characters only)
Status: disabled
Physical Interface: 1
Remote Address: 0.0.0.0

Host 1 Tunnel		Host 2 Tunnel	
Source IP:	0.0.0.0	Source IP:	0.0.0.0
Destination IP:	0.0.0.0	Destination IP:	0.0.0.0
Mask:	0.0.0.0	Mask:	0.0.0.0

Fields and buttons on the Network/GRE Tunnels Add new GRE Tunnel form are as follows:

- Add GRE Tunnel
  - □ Identifier provides a list to specify the numerical ID, between 1 and 5, for the GRE tunnel.
  - □ Name provides an entry field to specify the GRE tunnel name.
  - □ Status provides a list containing two selections:
    - o Disabled
    - o Enabled
  - □ Physical Interface provides a list to specify a numerical value between 1 and 255.
  - □ Remote Address provides an entry field to specify the remote IP address of the GRE tunnel.

- Host 1 Tunnel
  - Source IP provides an entry field for the tunnel source IP address for host 1.
  - Destination IP provides an entry field for the tunnel destination IP address for host 1.
  - Mask provides an entry field for the tunnel subnet mask.
- Host 2 Tunnel
  - Source IP provides an entry field for the tunnel source IP address for host 2.
  - Destination IP provides an entry field for the tunnel destination IP address for host 2.
  - Mask provides an entry field for the tunnel subnet mask.
- Update submits the changes to the pending configuration.
- Back returns to the Network/GRE Tunnels form without submitting changes to the pending configuration.

Status forms

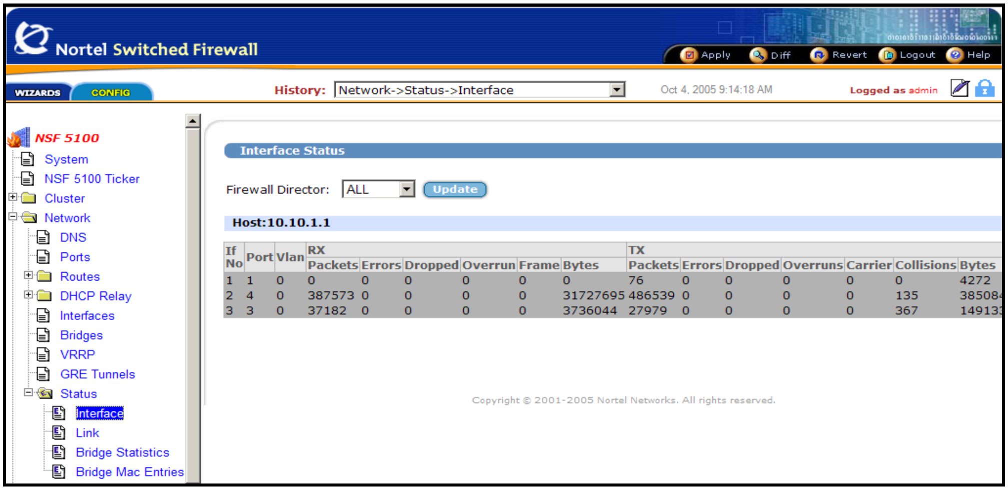
Following are four Network/Status forms:

- Interface (see Network/Status/Interface form)
- Link (see Network/Status/Link form on page 86)
- Bridge Statistics (see Network/Status/Bridge Statistics form on page 87)
- Bridge Mac Entries (see Network/Status/Bridge Mac Entries form on page 88)

Network/Status/Interface form

The Network/Status/Interface form provides runtime information for all Ethernet ports on the Firewall. Information includes errors, dropped packets, overruns, and frames for all transmitted and received packets, in addition to number of carriers and overruns for all transmitted (TX) packets (see Network/Status/Interface form). The Firewall Director list provides the option of selecting all or individual interfaces.

Figure 56 Network/Status/Interface form



History: Network->Status->Interface

Oct 4, 2005 9:14:18 AM

Logged as admin

Interface Status

Firewall Director: ALL

Update

Host:10.10.1.1

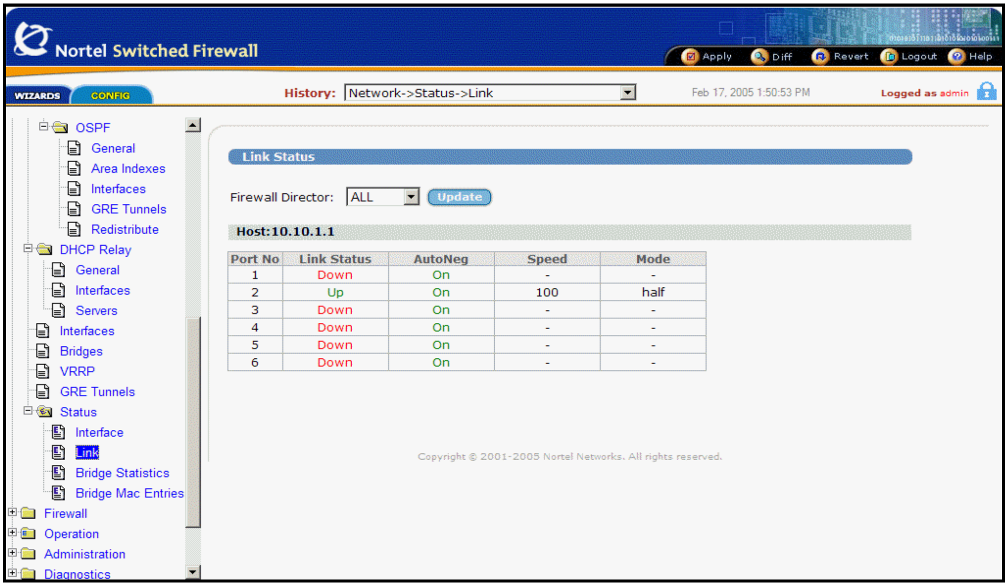
If No	Port	Vlan	RX						TX						
			Packets	Errors	Dropped	Overrun	Frame	Bytes	Packets	Errors	Dropped	Overruns	Carrier	Collisions	Bytes
1	1	0	0	0	0	0	0	0	76	0	0	0	0	0	4272
2	4	0	387573	0	0	0	0	31727695	486539	0	0	0	0	135	38508
3	3	0	37182	0	0	0	0	3736044	27979	0	0	0	0	367	14913

Copyright © 2001-2005 Nortel Networks. All rights reserved.

Network/Status/Link form

Use the Network/Status/Link form to obtain information about all network interface ports (see Network/Status/Link form).

Figure 57 Network/Status/Link form



History: Network->Status->Link

Feb 17, 2005 1:50:53 PM

Logged as admin

Link Status

Firewall Director: ALL

Host:10.10.1.1

Port No	Link Status	AutoNeg	Speed	Mode
1	Down	On	-	-
2	Up	On	100	half
3	Down	On	-	-
4	Down	On	-	-
5	Down	On	-	-
6	Down	On	-	-

Copyright © 2001-2005 Nortel Networks. All rights reserved.

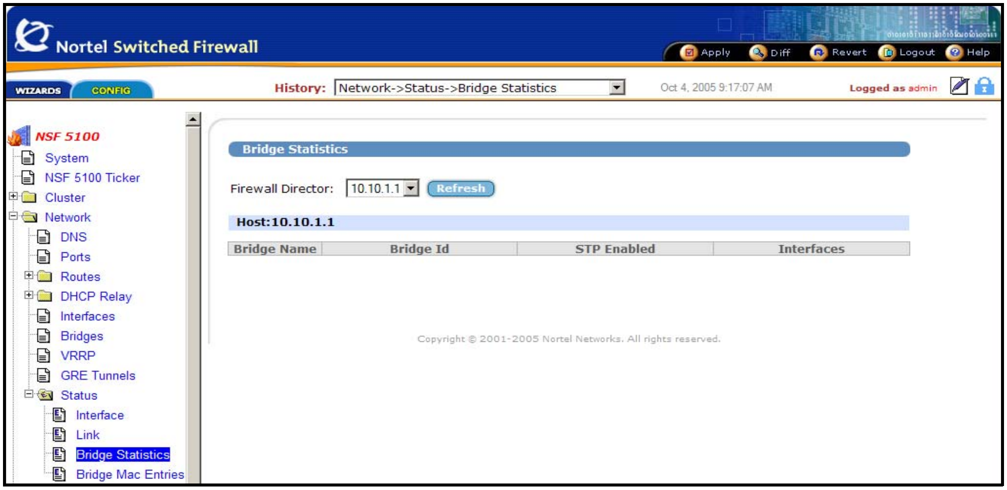
Fields and buttons on the Network/Status/Link form are as follows:

- Firewall Director provides a list of all hosts on the system. You can select ALL or individual hosts.
- Update provides information about the selected hosts.
- Port No. provides the port number on the selected host.
- Link Status displays the link as UP or DOWN.
- Autoneg specifies whether autonegotiation is set on the port.
- Speed specifies the link speed in Mbps as 10, 100, or 1000.
- Mode specifies the operating mode as Full Duplex or Half Duplex.

Network/Status/Bridge Statistics form

Use the Network/Status/Bridge Statistics form to view the bridge statistics for the selected firewall (see Network/Status/Bridge Statistics form).

Figure 58 Network/Status/Bridge Statistics form



History: Network->Status->Bridge Statistics

Oct 4, 2005 9:17:07 AM

Logged as admin

Bridge Statistics

Firewall Director: 10.10.1.1

Host:10.10.1.1

Bridge Name	Bridge Id	STP Enabled	Interfaces

Copyright © 2001-2005 Nortel Networks. All rights reserved.

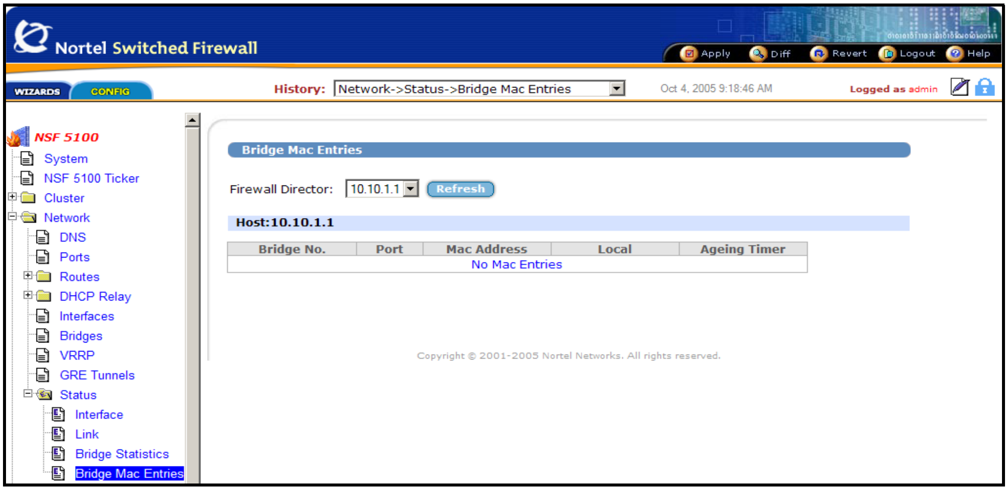
Fields and buttons on the Network/Status/Bridge Statistics form are as follows:

- Firewall Director provides a list of hosts in the system.
- Refresh provides the statistics for the selected host.
- Bridge Name specifies the name of the selected bridge.
- Bridge Id specifies the ID of the selected bridge.
- STP Enabled indicates whether or not STP is active.
- Interfaces provides statistics for the interfaces on the bridge.

Network/Status/Bridge Mac Entries form

Use the Network/Status/Bridge Mac Entries form to display the bridge MAC entries for the selected Firewall Director (see Network/Status/Bridge Mac Entries form).

Figure 59 Network/Status/Bridge Mac Entries form



History: Network->Status->Bridge Mac Entries

Oct 4, 2005 9:18:46 AM

Logged as admin

Bridge Mac Entries

Firewall Director: 10.10.1.1

Host:10.10.1.1

Bridge No.	Port	Mac Address	Local	Ageing Timer
No Mac Entries				

Copyright © 2001-2005 Nortel Networks. All rights reserved.

Fields and buttons on the Network/Status/Bridge Mac Entries form are as follows:

- Firewall Director provides a list to select the Firewall Director for bridge MAC entry display.
- Refresh provides the information for the selected Firewall Director.
- Bridge No. provides the numerical ID of the bridge.
- Port provides the port number of the bridge.
- Mac Address provides the MAC Address of the bridge.
- Local specifies whether the bridge is local.
- Ageing Timer displays the ageing timer.

Firewall forms

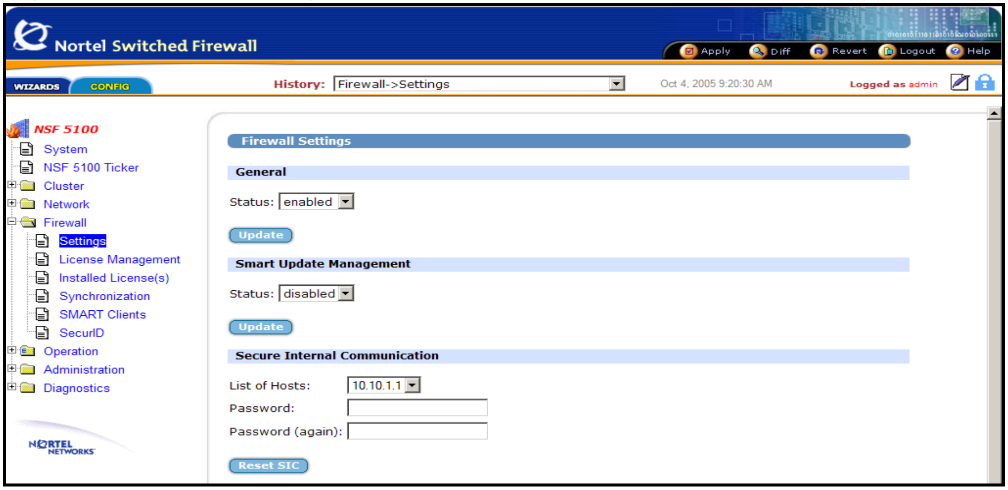
The Firewall menu includes the following five categories of forms:

- Settings (see Settings form)
- License Management (see License Management form on page 91)
- Installed Licenses (see Installed License(s) form on page 93)
- Synchronization (see Synchronization form on page 94)
- SMART Clients (see SMART Clients form on page 95)
- SecurID (see Firewall/SecurID form on page 96)

Settings form

Use the Firewall/Settings form to change the Firewall status and reset Secure Internal Communications (see Firewall/Settings form).

Figure 60 Firewall/Settings form



History: Firewall->Settings

Oct 4, 2005 9:20:30 AM

Logged as admin

Firewall Settings

General

Status: enabled

Smart Update Management

Status: disabled

Secure Internal Communication

List of Hosts: 10.10.1.1

Password:

Password (again):

The Firewall/Settings form is divided into three sections:

- General
- Smart Update Management
- Secure Internal Communication

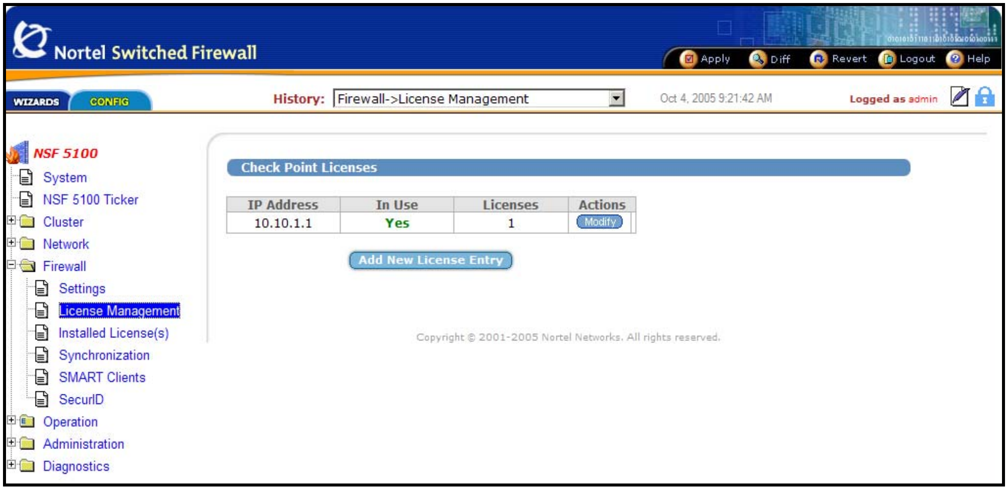
Fields and buttons on the form are as follows:

- General
    - Status provides a list with these selections:
        - Enabled indicates that Check Point FireWall-1 NGX is processing on the Firewall.
        - Disabled indicates that Check Point FireWall-1 NGX is not processing on the Firewall.
    - Update submits the changes to the pending configuration.
- Smart Update Management
    - Status provides a list with the following two selections:
        - Enabled indicates that Check Point SmartUpdate software updating is enabled. **TIP**: Disable SmartUpdate management when software update is complete.
        - Disabled indicates that Check Point SmartUpdate software updating is disabled.
    - Update submits the changes to the pending configuration.
- Secure Internal Communication is used to establish Secure Internal Communications (SIC) between the management station and the Firewall.
    - List of Hosts lists the Firewall hosts by IP address.
    - Password provides a field to enter the Check Point SIC password. **TIP**: This password differs from the login password.
    - Password (again) provides a field to reenter and confirm the Check Point SIC password.
    - Reset SIC resets SIC for the Firewall.

License Management form

Use the Firewall/Licenses form to modify or install additional Check Point licenses on the Firewall (see Firewall/License Management form).

Figure 61 Firewall/License Management form



History: Firewall->License Management

Check Point Licenses

IP Address	In Use	Licenses	Actions
10.10.1.1	Yes	1	Modify

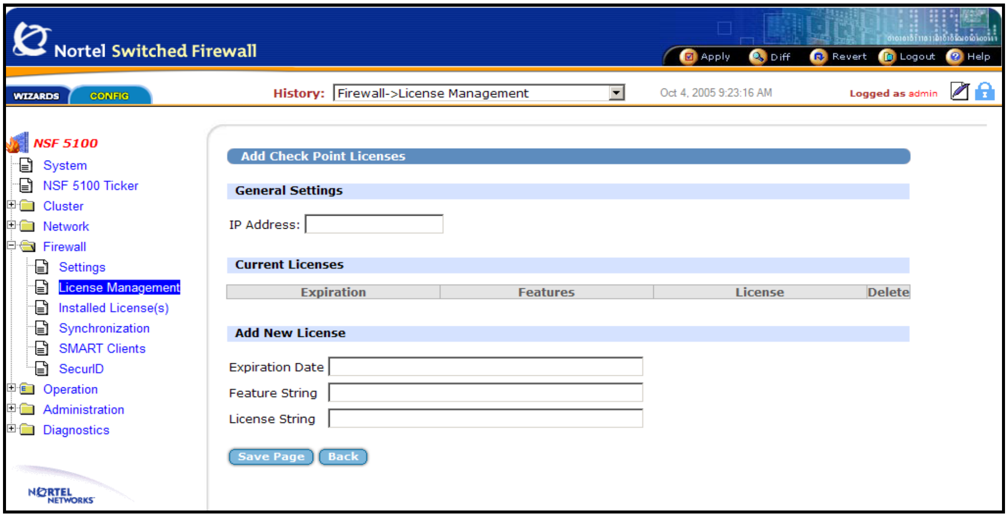
Fields and buttons on the Firewall/License Management form are as follows:

- IP Address is the address for the Firewall.
- In Use
  - Yes indicates that the IP address is currently assigned to a Firewall.
  - No indicates that the IP address is available to configure a new Firewall.
- Licenses shows the number of Check Point licenses currently configured for each IP address.
- Actions provides two choices, which are visible only if entries are present.
  - Click **Modify** to modify the Check Point licenses for the IP address.
  - Click **Delete** to delete the Check Point licenses for the IP address.
- Add New License Entry provides a form that permits addition of Check Point licenses for the IP address (see Firewall/License Management/Add New License Entry form on page 92).

Firewall/License Management/Add New License Entry form

Use the Firewall/License Management/Add New License Entry form to add Check Point licenses.

Figure 62 Firewall/License Management/Add New License Entry form



Add Check Point Licenses

General Settings

IP Address:

Current Licenses

Expiration	Features	License	Delete

Add New License

Expiration Date

Feature String

License String

The Firewall/License Management/Add New License Entry form is divided into three sections:

- General Settings
- Current Licenses
- Add New License

Fields and buttons on the form are as follows:

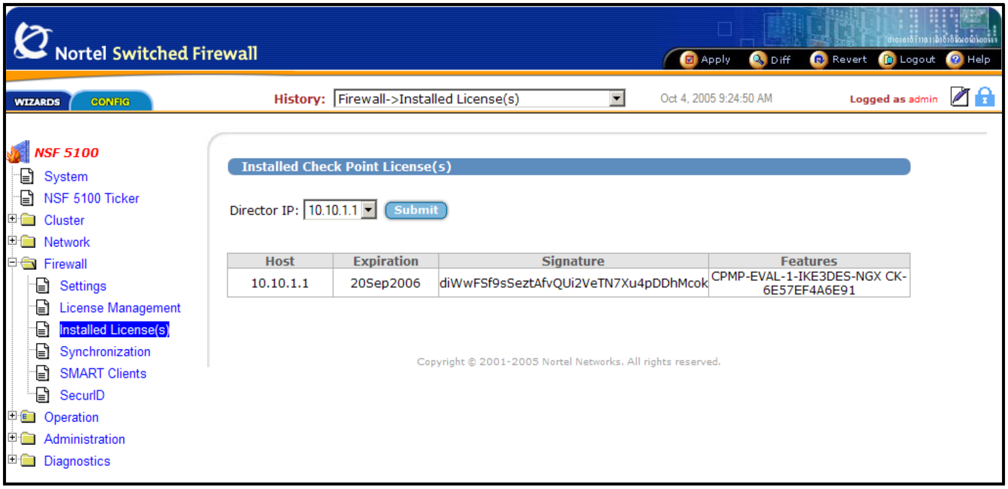
- General—IP Address provides an entry field to specify the host IP address associated with the new license.
- Current Licenses
  - Expiration provides an entry field to specify the Check Point License expiration date.
  - Features provides an entry field to specify the Check Point License feature string.
  - License provides an entry field to specify the Check Point License string.
  - Delete deletes the current license.

- Add New Licenses
  - □ Expiration Date provides an entry field to specify the Check Point License expiration date.
  - □ Feature String provides an entry field to specify the Check point License feature string.
  - □ License String provides an entry field to specify the Check Point License string.
  - □ Save Page submits the changes to the pending configuration.
  - □ Back returns to the Firewall/Licenses form without submitting changes to the pending configuration.

Installed License(s) form

Use the Firewall/Installed License(s) form to display information about current Check Point Licenses (see Firewall/Installed License(s) form).

Figure 63 Firewall/Installed License(s) form



History: Firewall->Installed License(s)

Oct 4, 2005 9:24:50 AM

Logged as admin

Installed Check Point License(s)

Director IP: 10.10.1.1 Submit

Host	Expiration	Signature	Features
10.10.1.1	20Sep2006	diWwFSf9sSeztAfvQUi2VeTN7Xu4pDDhMcok	CPMP-EVAL-1-IKE3DES-NGX CK-6E57EF4A6E91

Copyright © 2001-2005 Nortel Networks. All rights reserved.

Fields and buttons on the Firewall/Installed License(s) form are as follows:

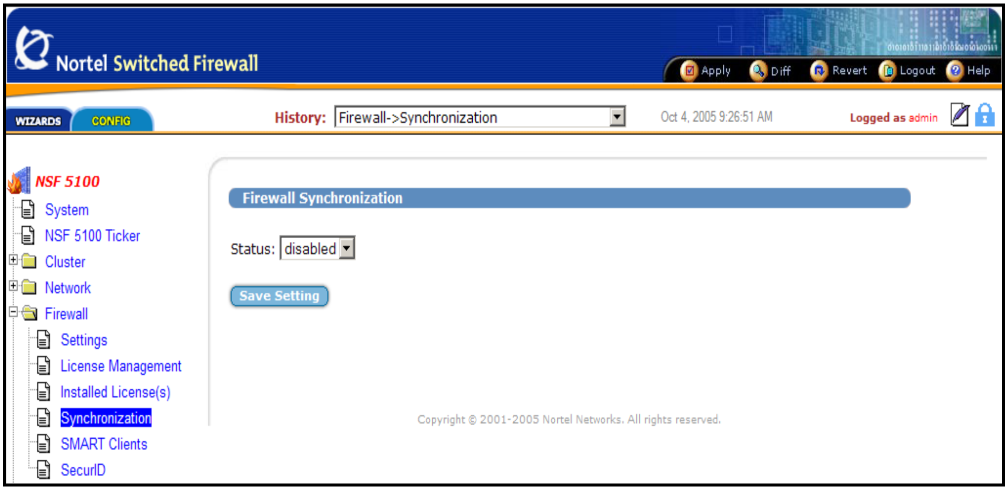
- Director IP provides a list of Director IP addresses.
  - □ Click **Submit** to request license information for the selected IP address.
- Host identifies the host associated with the license information.
- Expiration provides the license expiration date.
- Signature provides the Check Point License string.

- Features provides the Check Point license features.

Synchronization form

Use the Firewall/Synchronization form to display the cluster synchronization status and enable or disable cluster synchronization (see Firewall/Synchronization form).

Figure 64 Firewall/Synchronization form



History: Firewall->Synchronization

Oct 4, 2005 9:26:51 AM

Logged as admin

Status: disabled

NOTE – Firewall synchronization provides for stateful failover of open sessions when a master is backed up by the backup master.

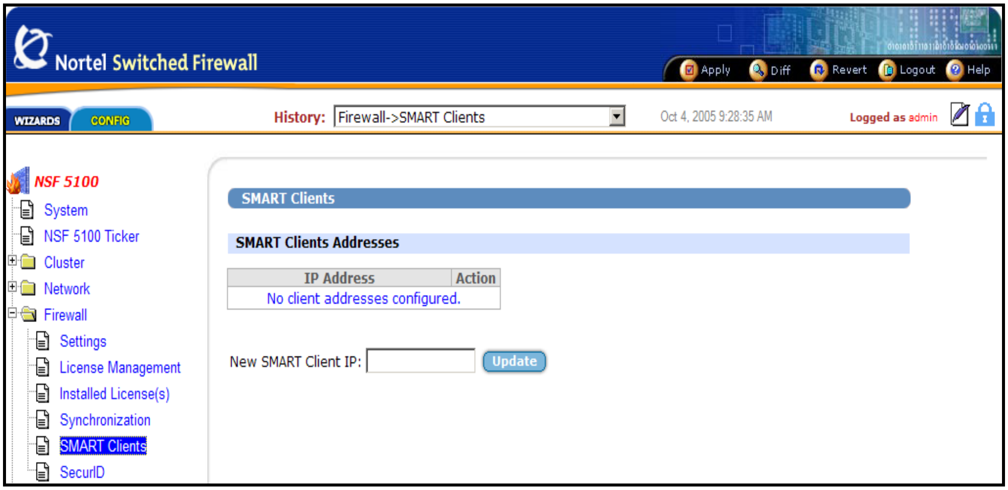
Fields and buttons on the Firewall/Synchronization form are as follows:

- Status displays a list providing two selections:
  - Enabled indicates that cluster synchronization is enabled.
  - Disabled indicates that cluster synchronization is disabled.
- Save Settings submits the changes to the pending configuration.

SMART Clients form

The Firewall/SMART Clients form displays, and allows modification to, SMART Clients addresses. This form also provides a field to add a new SMART Client (see Firewall/SMART Clients form).

Figure 65 Firewall/SMART Clients form



SMART Clients

SMART Clients Addresses

IP Address	Action
No client addresses configured.	

New SMART Client IP: Update

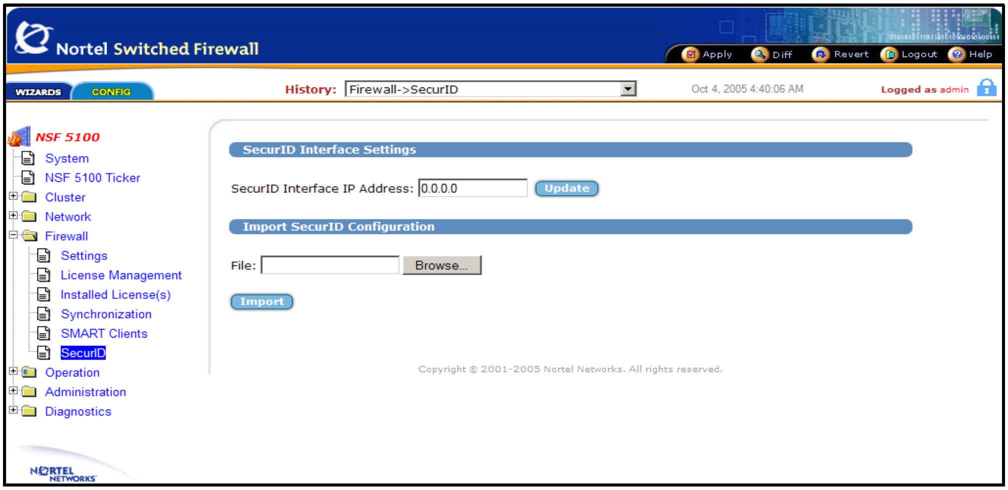
Fields and buttons on the Firewall/SMART Clients form are as follows:

- IP Address provides the IP Address of any configured SMART Clients.
- Action provides fields to delete or modify any present SMART Clients.
- New SMART Client IP provides a field to enter a new SMART Client IP address.
- Update submits the new SMART Client IP address to the pending configuration.

SecurID form

The SecurID form provides access to a two-factor form method for centralized authentication and management (see Firewall/SecurID form). For more information about SecurID, see the *Nortel Switched Firewall 5100 Series User's Guide and Command Reference* (213455-L).

Figure 66 Firewall/SecurID form



History: Firewall->SecurID

Oct 4, 2005 4:40:06 AM

Logged as admin

SecurID Interface Settings

SecurID Interface IP Address: 0.0.0.0

Import SecurID Configuration

File:

Copyright © 2001-2005 Nortel Networks. All rights reserved.

The SecurID form is divided into two sections.

Fields and buttons on the SecurID Interface Settings section are as follows:

- SecurID Interface IP Address specifies the Master Firewall external interface used to communicate with the SecurID server.
- Click **Update** to submit the SecurID interface address change to the pending configuration.

Fields and buttons on the Import SecurID Configuration section are as follows:

- File specifies the SecurID configuration file name. **TIP**: Click **Browse** to locate and select a file name.
- Click **Import** to import the SecurID configuration specified in the sdconf.rec file.

Operation forms

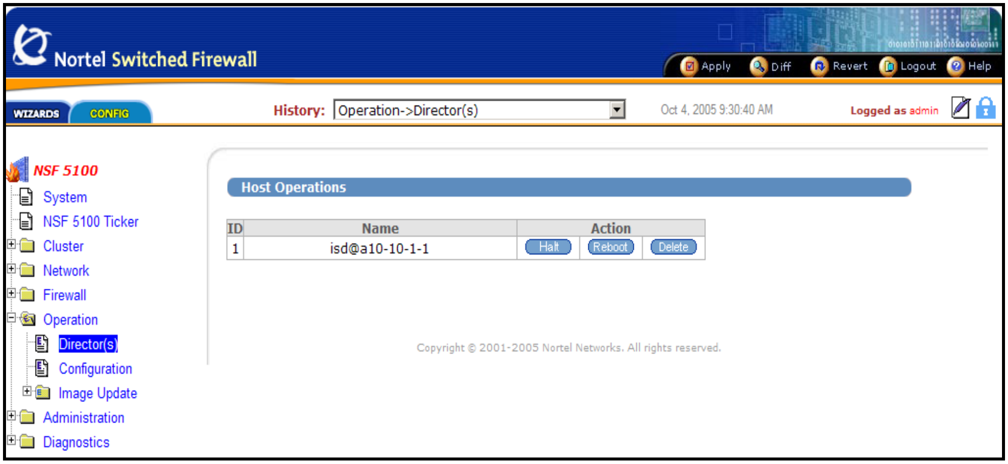
The Operation menu includes the following three categories of forms:

- Director(s) (see Director(s) form)
- Configuration (see Configuration form on page 98)
- Image Update (see Image Update forms on page 99)

Director(s) form

Use the Operation/Director(s) form to control the Firewall (see Operation/Director(s) form).

Figure 67 Operation/Director(s) form



History: Operation->Director(s)

Oct 4, 2005 9:30:40 AM

Logged as admin

ID	Name	Action		
1	isd@a10-10-1-1	Halt	Reboot	Delete

Copyright © 2001-2005 Nortel Networks. All rights reserved.

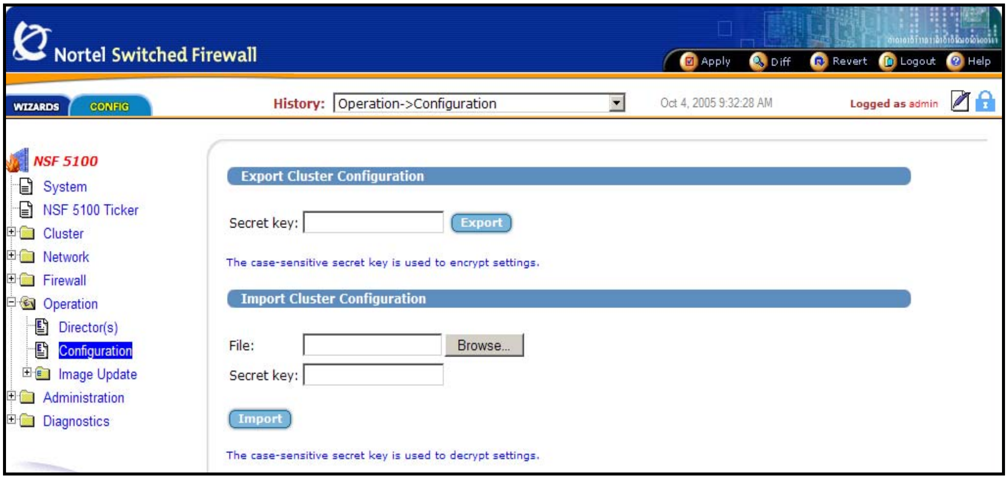
Fields and buttons on the Operation/Director(s) form are as follows:

- ID specifies the ID of any configured Firewall.
- Name describes the name and IP address of any configured Firewall.
- Action provides three management choices for the selected Firewall:
  - Halt stops operation of the Firewall.
  - Reboot shuts the Firewall down and restarts it.
  - Delete removes the Firewall from the configuration.

Configuration form

Use the Operation/Configuration form to export or import configuration files (see Operation/Configuration form).

Figure 68 Operation/Configuration form



History: Operation->Configuration

Oct 4, 2005 9:32:28 AM

Logged as admin

Export Cluster Configuration

Secret key:

The case-sensitive secret key is used to encrypt settings.

Import Cluster Configuration

File:

Secret key:

The case-sensitive secret key is used to decrypt settings.

The Operation/Configuration form is divided into two sections:

- Export Cluster Configuration
- Import Cluster Configuration

Fields and buttons on the form are:

- Export Cluster Configuration
  - Secret key provides a case-sensitive entry field to create a secret key used to encrypt the settings. **TIP:** The secret key must be supplied again when the configuration is imported.
    - Export is used to export the configuration. **TIP**: Depending on the browser type, the administrator can have the option to send output to a file or to the display. Output is sent to the display can be captured using Copy and Paste functions.
- Import Cluster Configuration
  - File provides a field to type in a configuration file name to import.
    - Browse provides access to a library of configuration files, if available, for selection of a configuration file to import.
  - Secret key provides a case-sensitive entry field. **TIP**: The import secret key is used to decrypt the configuration settings.

□ Import causes the BBI to restart immediately, using the replacement configuration. **TIP**: No **`Apply`** command is required in conjunction with Import.

WARNING – IMPORT CAUSES REPLACEMENT OF THE CURRENT CONFIGURATION, AND ALL PREVIOUS CONFIGURATION SETTINGS, BY THE IMPORTED CONFIGURATION. ALL CHANGES PENDING AT THE TIME OF THE IMPORT ARE LOST. THE REVERT COMMAND CANNOT BE USED TO RECOVER THE PREVIOUS CONFIGURATION.

Image Update forms

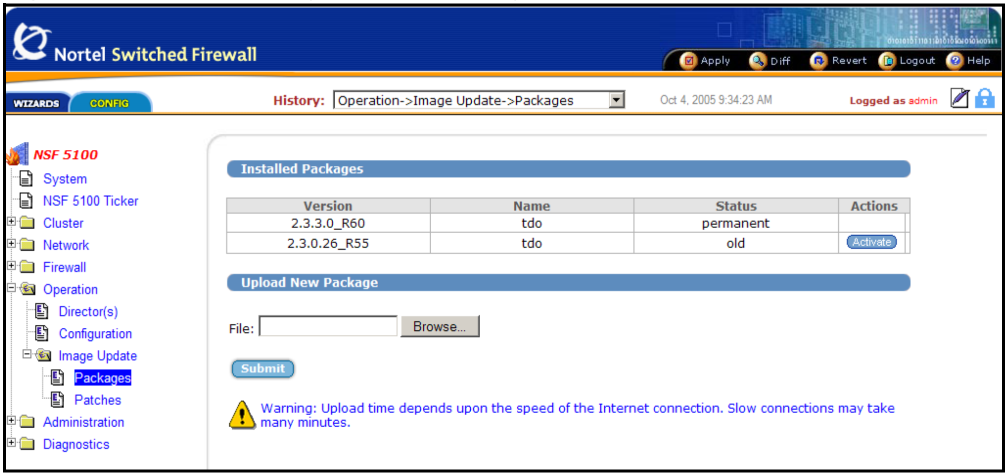
Operation/Image Update provides two forms:

- Packages (see Operation/Image Update/Packages form)
- Patches (see Operation/Image Update/Patches form on page 101)

Operation/Image Update/Packages form

Use the Operation/Image Update/Packages form to obtain information about software running on the firewall and to update the NSF software from the browser (see Operation/Image Update/Packages form).

Figure 69 Operation/Image Update/Packages form



History: Operation->Image Update->Packages

Oct 4, 2005 9:34:23 AM

Logged as admin

Installed Packages

Version	Name	Status	Actions
2.3.3.0_R60	tdo	permanent	
2.3.0.26_R55	tdo	old	Activate

Upload New Package

File: [ ] Browse...

Submit

Warning: Upload time depends upon the speed of the Internet connection. Slow connections may take many minutes.

The Operation/Image Update/Packages form is divided into the following two sections:

- Installed Packages
- Upload New Package

Fields and buttons on the Operation/Image Update/Packages form are as follows:

- Installed Packages
  - Version provides the NSF software version running on the cluster.
  - Name provides the name of the software package.
  - Status indicates software package status as follows:
    - permanent—the version that is currently running
    - old—the previous version is displayed if at least one version has been uploaded and activated
    - unpacked—a version downloaded, but not activated **TIP**: The code must be unpacked as part of the activation process.
  - Actions provides the following selections:
    - Activate reboots the Firewall host with the selected software version.
    - Delete removes the selected software version from storage.
- Upload New Package
  - File provides a field to enter a software package file name.
  - Browse provides navigation to the file location to select a file to upload.
  - Submit uploads the selected software package.

Browser-based software update

A browser-based software update differs from a CLI-based software update, because a TFTP or FTP server is not required to upload software.

To perform a browser-based software update, do the following:

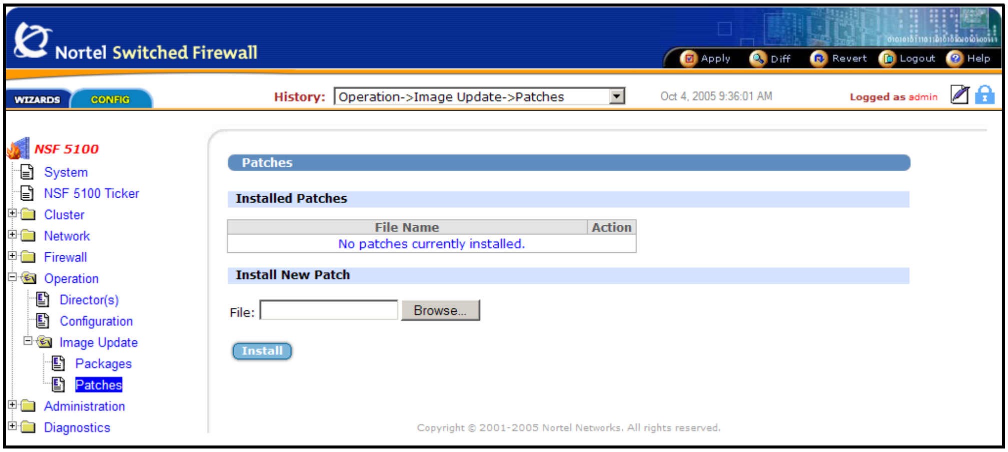
- Use the browser to locate and download the software update *.pkg* file from the Nortel web site to the Windows Desktop.
- Open the NSF BBI.
- Select the Operation/Image Update/Packages form and do the following:
  - To locate and select the software *.pkg* file, click **Browse** .
  - To load the latest software update on the Firewall, click **Submit** .

NOTE – Activating the software using the browser disables remote access to the Firewall. Use the local console to re-enter the Check Point License and reload the remote access policy to restore remote, or browser, access.

Operation/Image Update/Patches form

Use the Operation/Image Update/Patches form to obtain information about existing patches and to install or uninstall patches (see Operation/Image Update/Patches form).

Figure 70 Operation/Image Update/Patches form



File Name	Action
No patches currently installed.	

The Operation/Image Update/Patches form is divided into the following two sections:

- Installed Patches
- Install New Patch

Fields and buttons on the form are as follows:

- Installed patches
  - File Name provides the file name of patches installed on the system.
  - Action provides an Un-install button to remove the selected patch.
- Install New Patch
  - File provides an entry field to record the name of a patch to install.
  - Click **Browse** to view patch file names to select.
  - Click **Install** to install the selected patch.

Administration forms

The Administration forms provide access to administering and monitoring aspects of the Firewall, such as user information, web settings, and SNMP activity.

The Administration forms menu includes the following categories of forms:

- Monitor (see Monitor forms)
- Users (see Users forms on page 110)
- Access List (see Access List form on page 115)
- Telnet-SSH (see Telnet-SSH form on page 117)
- Web (see Web forms on page 118)
- SNMP (see SNMP forms on page 126)
- SSH Keys (see SSH Keys form on page 135)
- RADIUS (see RADIUS form on page 138)
- APC UPS (see APC UPS form on page 141)
- Audit (see Audit form on page 142)

Monitor forms

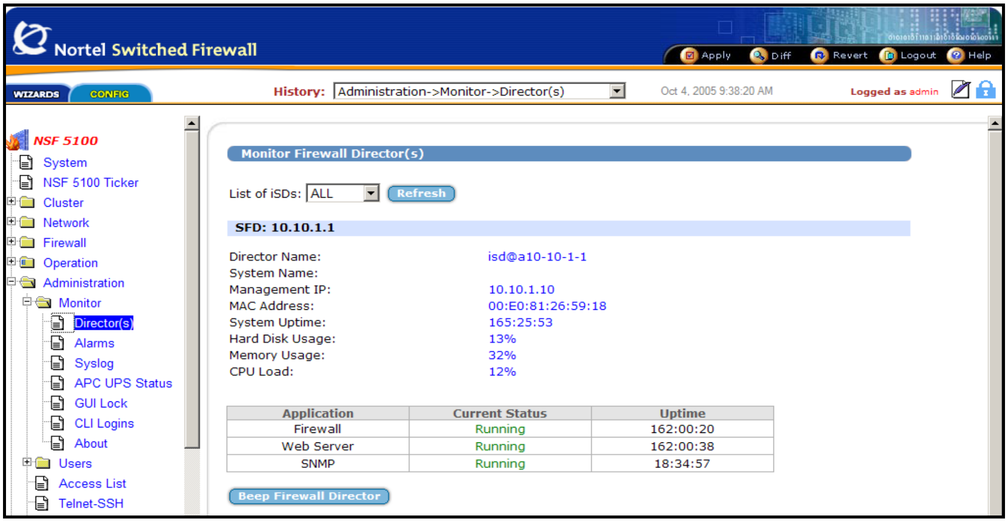
Administration/Monitor provides the following seven forms for monitoring aspects of Firewall health and operation:

- Director(s) (see Administration/Monitor/Director(s) form on page 103)
- Alarms (see Administration/Monitor/Alarms form on page 104)
- Syslog (see Administration/Monitor/Syslog form on page 105)
- APC UPS Status (see Administration/Monitor/APC UPS Status form on page 106)
- GUI Lock (see Administration/Monitor/GUI Lock form on page 107)
- CLI Logins (see Administration/Monitor/CLI Logins form on page 108)
- About (see Administration/Monitor/About form on page 109)

Administration/Monitor/Director(s) form

The Administration/Monitor/Director(s) form displays Firewall director details and application status (see Administration/Monitor/Director(s) form).

Figure 71 Administration/Monitor/Director(s) form



History: Administration->Monitor->Director(s)

Oct 4, 2005 9:38:20 AM

Logged as admin

Monitor Firewall Director(s)

List of iSDs: ALL

SFD: 10.10.1.1

Director Name:	isd@a10-10-1-1
System Name:	
Management IP:	10.10.1.10
MAC Address:	00:E0:81:26:59:18
System Uptime:	165:25:53
Hard Disk Usage:	13%
Memory Usage:	32%
CPU Load:	12%

Application	Current Status	Uptime
Firewall	Running	162:00:20
Web Server	Running	162:00:38
SNMP	Running	18:34:57

Fields and buttons on the Administration/Monitor/Director(s) form are as follows:

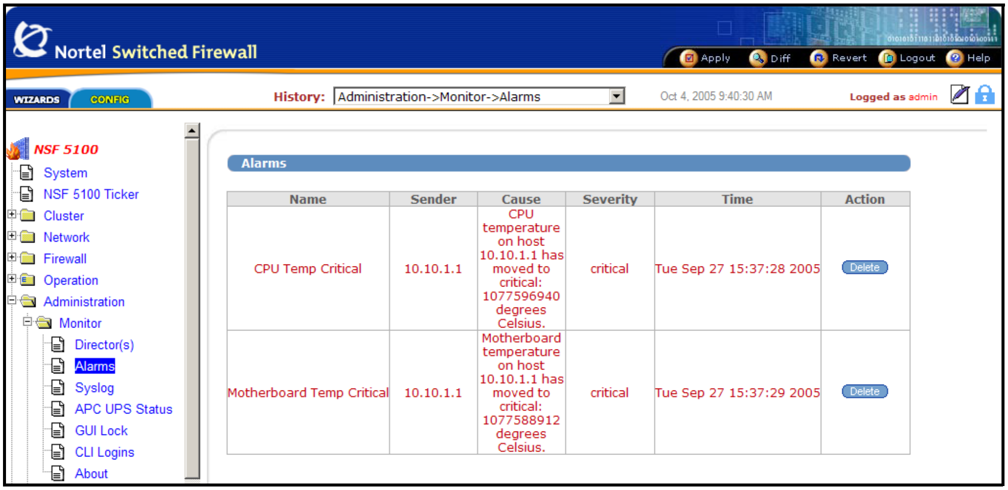
- List of iSDs provides a list containing individual iSD selections or ALL.
  - Refresh updates the display with the details for the selection from the list of iSDs.
- Director Name provides the name of the Firewall Director.
- System Name provides the designated name of the system.
- Management IP provides the Management IP (MIP) of the Firewall.
- MAC Address provides the MAC address of the Firewall.
- System Uptime provides the time, in Hours:Minutes:Seconds, since the last boot of the Firewall.
- Hard Disk Usage provides the percentage of hard disk space used on the Firewall.
- Memory Usage provides the percentage of memory used on the Firewall.
- CPU Load provides the percentage of CPU used on the Firewall.
- Application provides a list of the current applications running on the Firewall.
- Current Status provides the current status of the applications: running or disabled.

- Uptime provides the time, in Hours:Minutes:Seconds, since the applications started.
- To help determine which physical host is using a particular IP Address, click **Beep Firewall Director** to cause multiple beeps to be emitted at the host.

Administration/Monitor/Alarms form

The Administration/Monitor/Alarms form provides information about alarm status (see Administration/Monitor/Alarms form).

Figure 72 Administration/Monitor/Alarms form



History: Administration->Monitor->Alarms

Oct 4, 2005 9:40:30 AM

Logged as admin

Alarms

Name	Sender	Cause	Severity	Time	Action
CPU Temp Critical	10.10.1.1	CPU temperature on host 10.10.1.1 has moved to critical: 1077596940 degrees Celsius.	critical	Tue Sep 27 15:37:28 2005	Delete
Motherboard Temp Critical	10.10.1.1	Motherboard temperature on host 10.10.1.1 has moved to critical: 1077588912 degrees Celsius.	critical	Tue Sep 27 15:37:29 2005	Delete

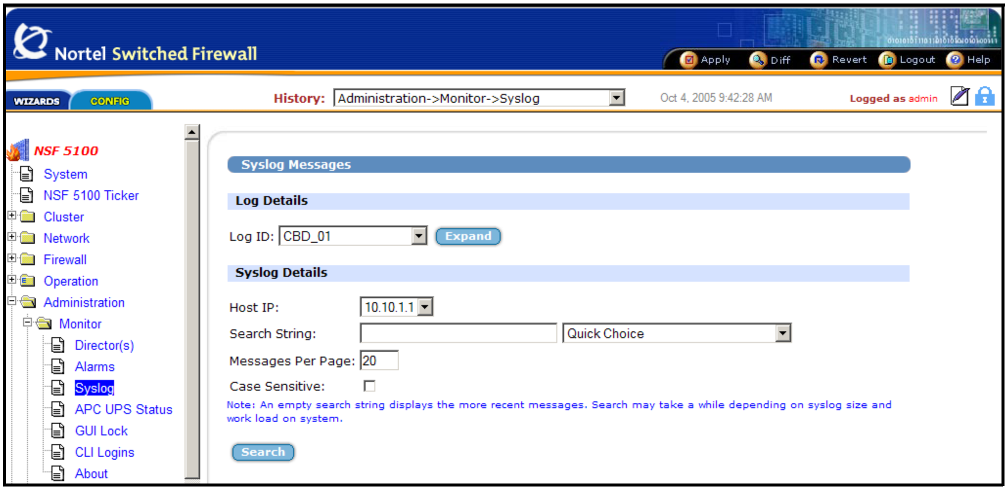
Fields and buttons on the Administration/Monitor/Alarms form are as follows:

- Name provides the name of the alarm.
- Sender provides the IP address of the alarm source.
- Cause describes the cause of the alarm.
- Severity provides the severity level of the alarm:
  - Critical
  - Major
  - Minor
  - Warning
- Time provides the time the event occurred.
- Action permits deletion of the selected alarm.

Administration/Monitor/Syslog form

The Administration/Monitor/Syslog form displays the system logs for the Firewall based on selected search criteria (see Administration/Monitor/Syslog form).

Figure 73 Administration/Monitor/Syslog form



Log ID: CBD_01

Host IP: 10.10.1.1

Search String: Quick Choice

Messages Per Page: 20

Case Sensitive: □

Note: An empty search string displays the more recent messages. Search may take a while depending on syslog size and work load on system.

The Administration/Monitor/Syslog form is divided into the following two sections:

- Log Details
- Syslog Details

Fields and buttons on the form are as follows:

Log Details

- Log ID provides a list containing names of existing log IDs. Expand provides the log details for the selected Log ID.

Syslog Details

- Host IP provides a list of Firewall IP addresses that have logs.
- Search String provides an entry field to specify a string to search for the message body. **TIP**: All messages with a substring matching the characters in this field are displayed if **Search** is selected.
- Quick Choice is a list that provides a list of predefined basic search strings as follows:
  - All critical messages (CRITICAL)
  - All error messages (ERROR)

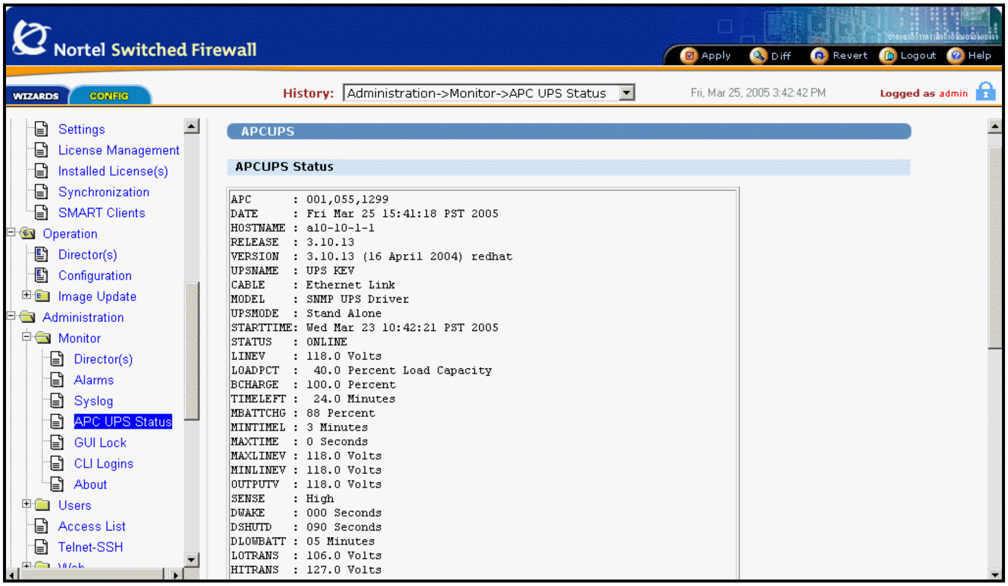
  - □ All info messages (INFO)
  - □ All notice messages (NOTICE)
  - □ All warning messages (WARNING)

- Messages Per Page provides the maximum number of messages displayed for each request.
- Case Sensitive provides a check box to select or deselect case sensitivity in the search.
- Search executes the log search using the defined parameters. **TIP**: When the search is complete, a list of messages matching the search criterion appears at the bottom of the form.

Administration/Monitor/APC UPS Status form

The Administration/Monitor/APC UPS Status form provides information about status of the American Power Corporation uninterrupted power supply (APC UPS) (see Administration/Monitor/APC UPS Status form).

Figure 74 Administration/Monitor/APC UPS Status form



History: Administration->Monitor->APC UPS Status

Fri, Mar 25, 2005 3:42:42 PM

Logged as admin

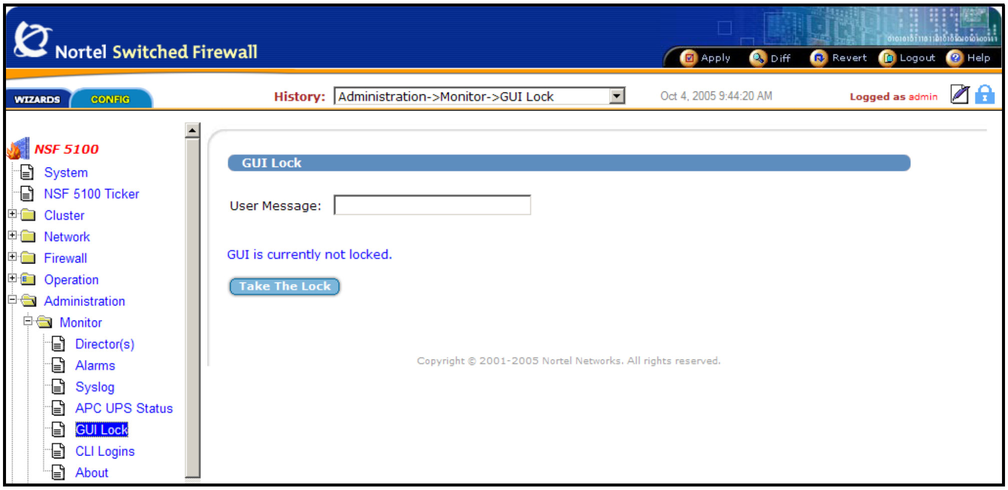
APCUPS Status

```
APC      : 001,055,1299
DATE     : Fri Mar 25 15:41:18 PST 2005
HOSTNAME : a10-10-1-1
RELEASE  : 3.10.13
VERSION  : 3.10.13 (16 April 2004) redhat
UPSNAME  : UPS KEV
CABLE    : Ethernet Link
MODEL    : SNMP UPS Driver
UPSMODE  : Stand Alone
STARTTIME: Wed Mar 23 10:42:21 PST 2005
STATUS   : ONLINE
LINEV    : 118.0 Volts
LOADPCT  :  40.0 Percent Load Capacity
BCHARGE  : 100.0 Percent
TIMELEFT :  24.0 Minutes
MBATTCHG : 88 Percent
MINTIMEL : 3 Minutes
MAXTIME  : 0 Seconds
MAXLINEV : 118.0 Volts
MINLINEV : 118.0 Volts
OUTPUTV  : 118.0 Volts
SENSE    : High
DWAKE    : 000 Seconds
DSHUTD   : 090 Seconds
DLOWBATT : 05 Minutes
LOTRANS  : 106.0 Volts
HITRANS  : 127.0 Volts
```

Administration/Monitor/GUI Lock form

The Administration/Monitor/GUI Lock form allows an administrator to take control of the GUI lock and provide an alert message to other users (see Administration/Monitor/GUI Lock form). Taking control of the GUI lock prevents firewall configuration conflicts between concurrent user sessions.

Figure 75 Administration/Monitor/GUI Lock form



History: Administration->Monitor->GUI Lock

Oct 4, 2005 9:44:20 AM

Logged as admin

GUI Lock

User Message:

GUI is currently not locked.

Copyright © 2001-2005 Nortel Networks. All rights reserved.

Fields and buttons on the Administration/Monitor/GUI Lock form are as follows:

- User Message provides an entry field for the administrator taking control of the GUI lock to create a message. This message displays to other administrators until the controller of the lock releases it.
- to take control of the GUI lock, click **Take The Lock** . The Lock form appears.

Fields and buttons on the Lock form are as follows:

- User Name provides an entry field to specify the name of the administrator who has taken control of the GUI lock.
- Lock Time provides an entry field to specify the time the GUI lock was taken.

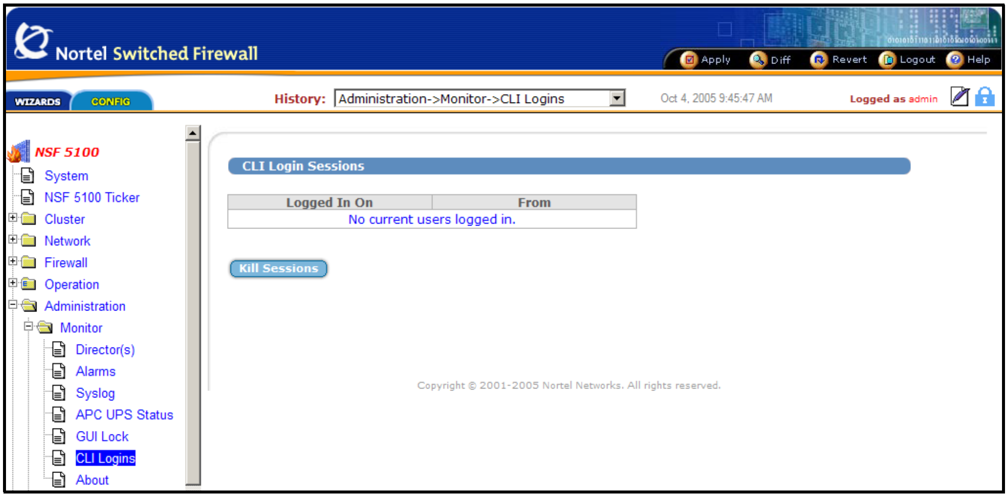
Return to the Lock form to release the lock and do the following:

- To release the GUI lock before closing the current session, click **Release The Lock**.

Administration/Monitor/CLI Logins form

The Administration/Monitor/CLI Logins form provides information about CLI Login sessions on the Firewall (see Administration/Monitor/CLI Logins form).

Figure 76 Administration/Monitor/CLI Logins form



History: Administration->Monitor->CLI Logins

Oct 4, 2005 9:45:47 AM

Logged as admin

CLI Login Sessions

Logged In On	From
No current users logged in.	

Copyright © 2001-2005 Nortel Networks. All rights reserved.

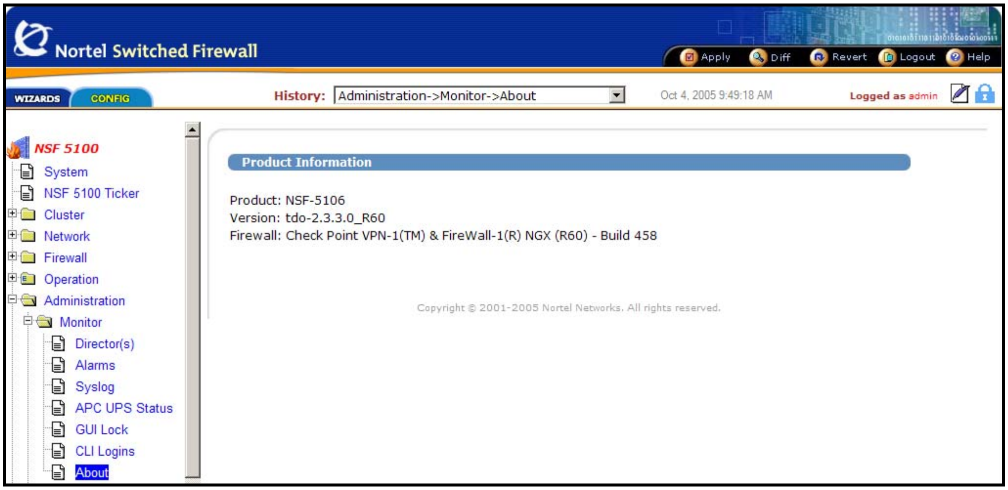
Fields and buttons on the Administration/Monitor/CLI Logins form are as follows:

- Logged In On specifies the time the user logged in to the CLI.
- From specifies the IP address of the remote user.
- Kill Sessions terminates all CLI sessions.

Administration/Monitor/About form

The Administration/Monitor/About form displays general product information about the Firewall (see Administration/Monitor/About form).

Figure 77 Administration/Monitor/About form



Product: NSF-5106
Version: tdo-2.3.3.0_R60
Firewall: Check Point VPN-1(TM) & FireWall-1(R) NGX (R60) - Build 458

Copyright © 2001-2005 Nortel Networks. All rights reserved.

Fields and buttons on the Administration/Monitor/About form are as follows:

- Product provides the model number of the cluster that is connected to the BBI.
- Version provides the software version running on the cluster.
- Firewall provides the Check Point software build and feature pack running on the cluster.

Users forms

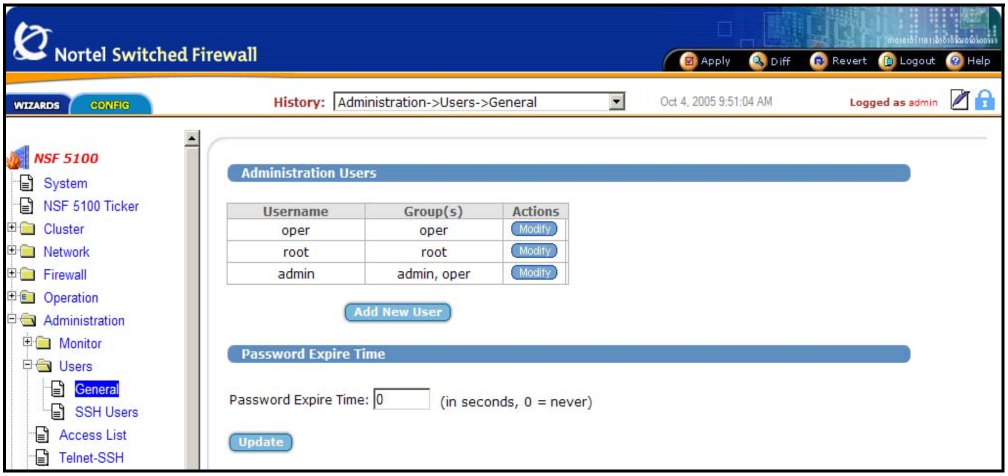
Administration/Users provides the following two categories of forms:

- General (see Administration/Users/General form)
- SSH Users (see Administration/Users/SSH Users form on page 113)

Administration/Users/General form

Use the Administration/Users/General form to add, modify, delete, or list Firewall user accounts, and change passwords (see Administration/Users/General form).

Figure 78 Administration/Users/General form



History: Administration->Users->General

Oct 4, 2005 9:51:04 AM

Logged as admin

Administration Users

Username	Group(s)	Actions
oper	oper	Modify
root	root	Modify
admin	admin, oper	Modify

Password Expire Time

Password Expire Time: 0 (in seconds, 0 = never)

The Administration/Users/General form is divided into the following two sections:

- Administration Users
- Password Expire Time

Fields and buttons on the form are as follows:

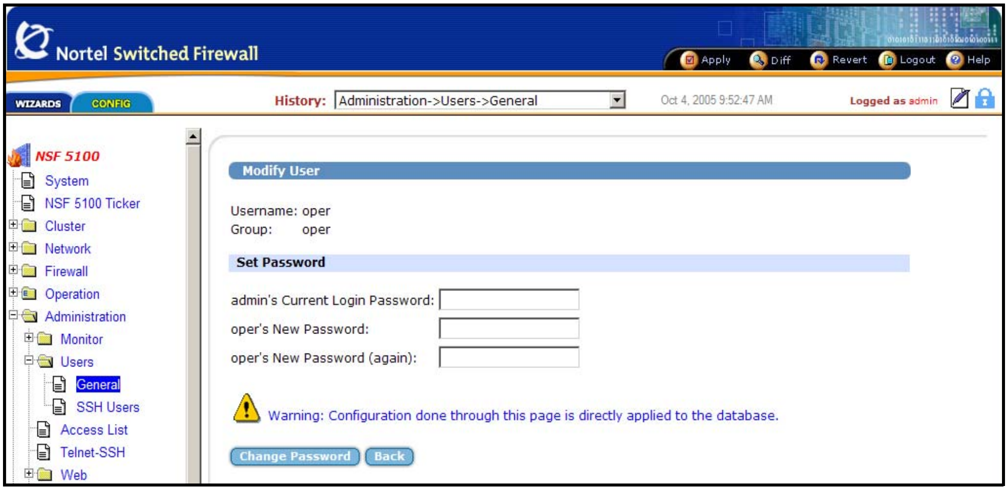
- Administration Users
  - □ Username provides the following default user names. **TIP**: You cannot remove the default names.
    - o oper user is a member of the Oper Group and has read access to the NSF.
    - o root is a member of the Root Group and has read/write access to the NSF.
    - o admin is a member of Admin and Oper Groups and has read/write access to the NSF.

  - □ Group(s) displays the group to which the user belongs.
  - □ Actions provides a Modify button used to modify passwords for the default user names or modify information for user names other than the defaults (see Administration/Users/General Modify User form).
  - □ Add New User provides access to the Add New User form used to add a new user name to a specified group and set the password (see Administration/Users/General Add New User form on page 112).
- Password Expire Time
  - □ Password Expire Time provides an entry field to set the password expiry time, in seconds, for the current user name. **TIP**: The password does not expire if the default value of 0 is used.
  - □ Update confirms the password expiration value set for the current user name.

Administration/Users/General Modify User form

Use the Administration/Users/General Modify User form to change the password for a specific user (see Administration/Users/General Modify User form).

Figure 79 Administration/Users/General Modify User form



Modify User

Username: oper
Group: oper

Set Password

admin's Current Login Password:
oper's New Password:
oper's New Password (again):

Warning: Configuration done through this page is directly applied to the database.

Change Password | Back

Fields and buttons on the Administration/Users/General/Modify User form are as follows:

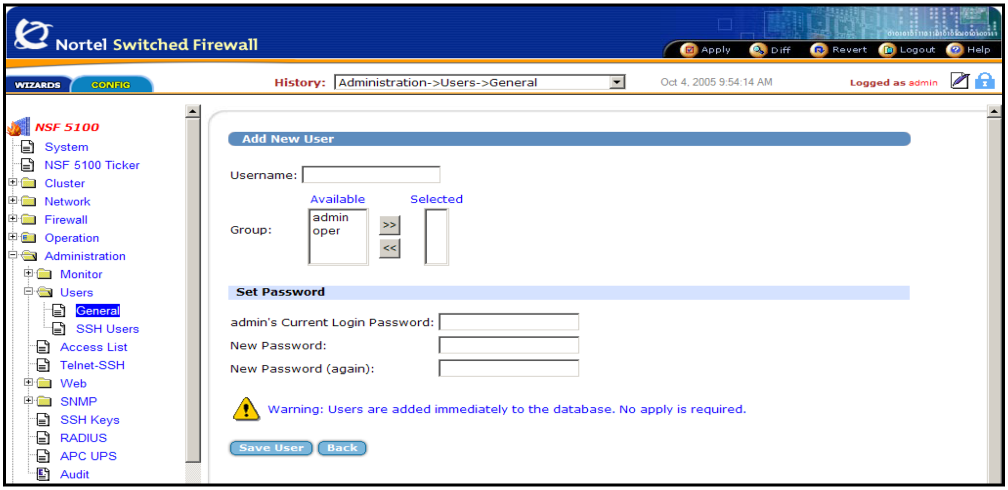
- Username provides the username.
- Group provides the name of the group to which the user is assigned.

- Current Login Password provides an entry field to record the current active password for the named user (for example, oper user or admin user).
- Password provides an entry field to record the new password.
- Password (again) provides an entry field to confirm the new password.
- Click **Change Password** to submit the new password to the pending configuration.
- Click **Back** to return to the Administration/Users/General form without submitting changes to the pending configuration.

Administration/Users/General Add New User form

Use the Administration/Users/General Add New User form to add new users (see Administration/Users/General Add New User form).

Figure 80 Administration/Users/General Add New User form



History: Administration->Users->General

Oct 4, 2005 9:54:14 AM

Logged as admin

Warning: Users are added immediately to the database. No apply is required.

Fields and buttons on the Administration/Users/General Add New User form are as follows:

- Add New User
  - □ Username provides an entry field to specify an identifier for the user.
  - □ Group provides a selection list to specify the group for the user.
- Set Password
  - □ Current Login Password provides an entry field to specify the login password for the administrator.
  - □ Password provides an entry field to specify a new password.

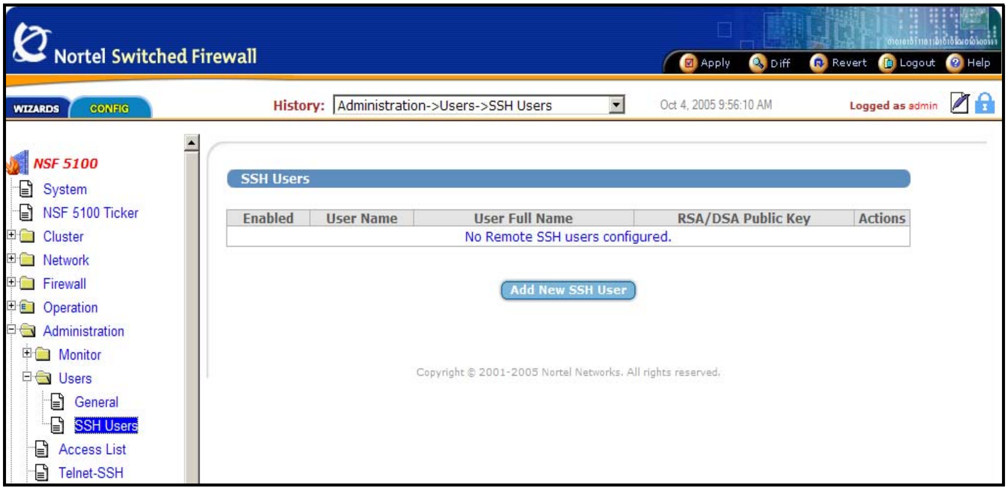
- □ Password (again) provides an entry field to confirm the new password.

- Save User saves the user information and returns to the Administration/users/General form. **TIP**: Save User applies the change. Do not use the Apply command.
- Back returns to the Administration/Users/General form with saving the user information.

Administration/Users/SSH form

Use the Administration/Users/SSH Users form to obtain and modify information about SSH users and to add new SSH Users (see Administration/Users/SSH Users form).

Figure 81 Administration/Users/SSH Users form



History: Administration->Users->SSH Users

Oct 4, 2005 9:56:10 AM

Logged as admin

SSH Users

Enabled	User Name	User Full Name	RSA/DSA Public Key	Actions

No Remote SSH users configured.

Copyright © 2001-2005 Nortel Networks. All rights reserved.

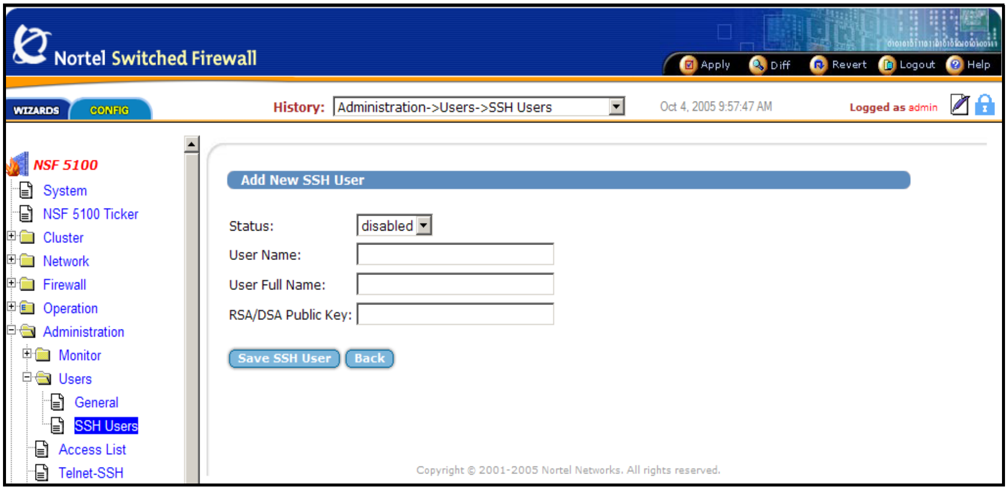
Fields and buttons on the Administration/Users/SSH Users form are as follows:

- Enabled specifies the status of the SSH user account.
- User Name specifies the name of the remote SSH user.
- User Full Name specifies the descriptive name of the remote SSH user.
- RSA/DSA Public Key specifies the public key used for RSA and DSA authentication.
- Actions provides the following two options:
  - □ Modify provides fields to modify the selected SSH user.
  - □ Delete deletes the selected SSH user.
- Add New SSH User (see Administration/Users/SSH Users Add New SSH User form on page 114).

Administration/Users/SSH Users Add New SSH User form

Use the Administration/Users/SSH Users Add New SSH User form to add a new SSH user to the configuration.

Figure 82 Administration/Users/SSH Users Add New SSH User form



Status: disabled

User Name:

User Full Name:

RSA/DSA Public Key:

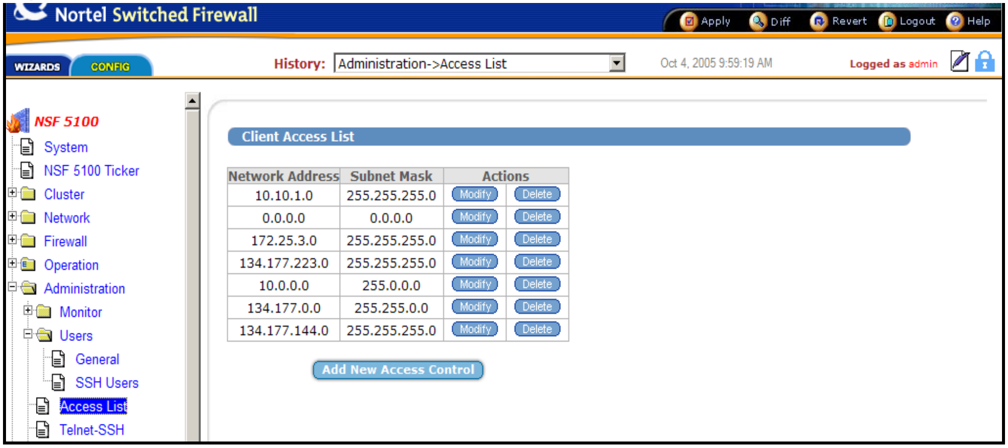
Fields and buttons on the Administration/Users/SSH Users Add New SSH User form are as follows:

- Status provides a list with the following two selections:
  - Enabled enables the SSH user.
  - Disabled disables the SSH user.
- User Name provides an entry field to specify the name of the remote SSH user.
- User Full Name provides an entry field to specify the descriptive name of the remote SSH user.
- RSA/DSA Public Key provides an entry field to specify the public key.
- Save SSH User saves the changes to the pending configuration.
- Back returns to the Administration/Users SSH Users form without submitting changes to the pending configuration.

Access List form

Use the Administration Access List form to specify which clients are permitted to administer the system (see Administration/Access List form). Web access must also be specified (see Administration/Web/General form on page 118).

Figure 83 Administration/Access List form



History: Administration->Access List

Oct 4, 2005 9:59:19 AM

Logged as admin

Client Access List

Network Address	Subnet Mask	Actions	
10.10.1.0	255.255.255.0	Modify	Delete
0.0.0.0	0.0.0.0	Modify	Delete
172.25.3.0	255.255.255.0	Modify	Delete
134.177.223.0	255.255.255.0	Modify	Delete
10.0.0.0	255.0.0.0	Modify	Delete
134.177.0.0	255.255.0.0	Modify	Delete
134.177.144.0	255.255.255.0	Modify	Delete

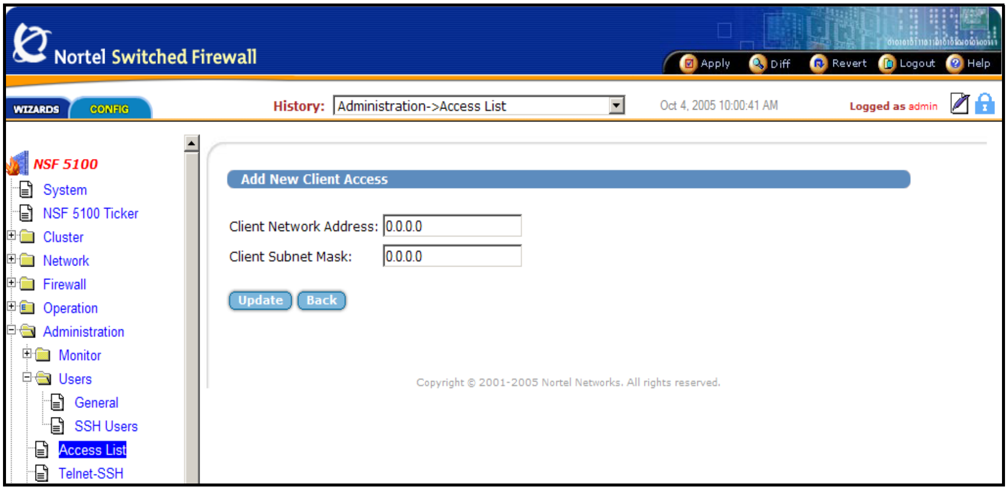
Fields and buttons on the Administration/Access List form are as follows:

- Network Address provides the IP address of the client.
- Subnet Mask provides the subnet address used for matching.
- Actions provides two buttons:
  - Modify displays a form to modify client information.
  - Delete deletes the selected entry. **TIP**: Deletion terminates the connection.
- Add New Access Control displays the Administration/Access List/Add form (see Administration/Access List Add New Client Access form on page 116).

Administration/Access List Add New Client Access form

Use the Administration/Access List Add New Client Access form to add a new client access to the configuration.

Figure 84 Administration/Access List Add New Client Access form



History: Administration->Access List

Oct 4, 2005 10:00:41 AM

Logged as admin

Client Network Address: 0.0.0.0

Client Subnet Mask: 0.0.0.0

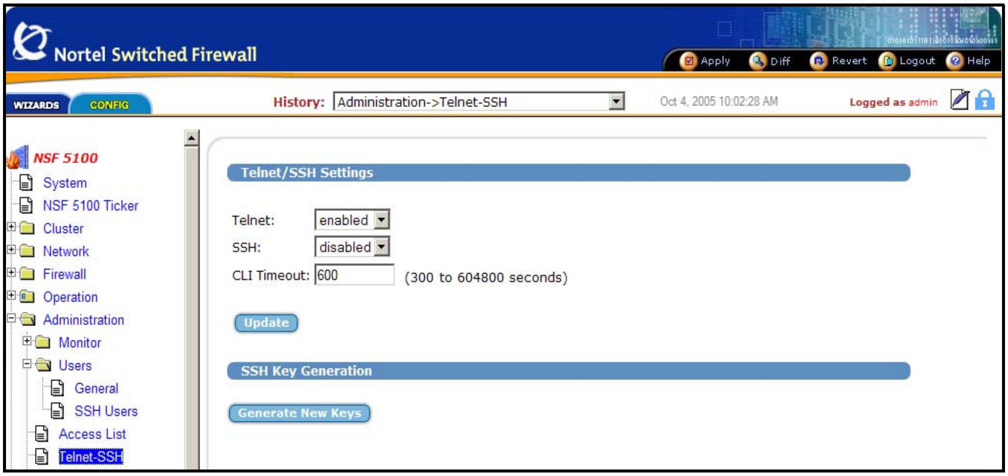
Fields and buttons on the Administration/Access List Add New Client Access form are as follows:

- Client Network Address provides an entry field to record the new client address.
- Client Subnet Mask provides an entry field to record the new client subnet mask.
- Click **Update** to submit the new client access information to the pending configuration.
- Click **Back** to return to the Administration/Access List without submitting changes to the pending configuration.

Telnet-SSH form

Use the Administration/Telnet-SSH form to enable or disable Telnet/SSH administration (see Administration/Telnet-SSH form).

Figure 85 Administration/Telnet-SSH form



History: Administration->Telnet-SSH

Oct 4, 2005 10:02:28 AM

Logged as admin

Telnet/SSH Settings

Telnet: enabled

SSH: disabled

CLI Timeout: 600 (300 to 604800 seconds)

SSH Key Generation

The Administration/Telnet-SSH form is divided into the following two sections:

- Telnet/SSH Settings
- SSH Key Generation

Fields and buttons on the form are as follows:

- Telnet/SSH Settings
  - Telnet enables or disables administration through Telnet.
  - SSH enables or disables administration through SSH.
  - CLI Timeout sets the number of seconds a Telnet or SSH session can remain idle before automatic disconnection. **TIP**: Changes to the Firewall configuration that are not applied before the CLI times out will be lost.
  - Update submits the form changes to the pending configuration.
- SSH Key Generation
  - Generate New Keys generates new SSH keys.

Web forms

The Administration/Web forms provide the following:

- Web (HTTP) administration
- Creation and administration of self-signed server certificates that allow the BBI to run under SSL
- Administration of server certificates on the host
- Administration of Certificate Authority (CA) certificates

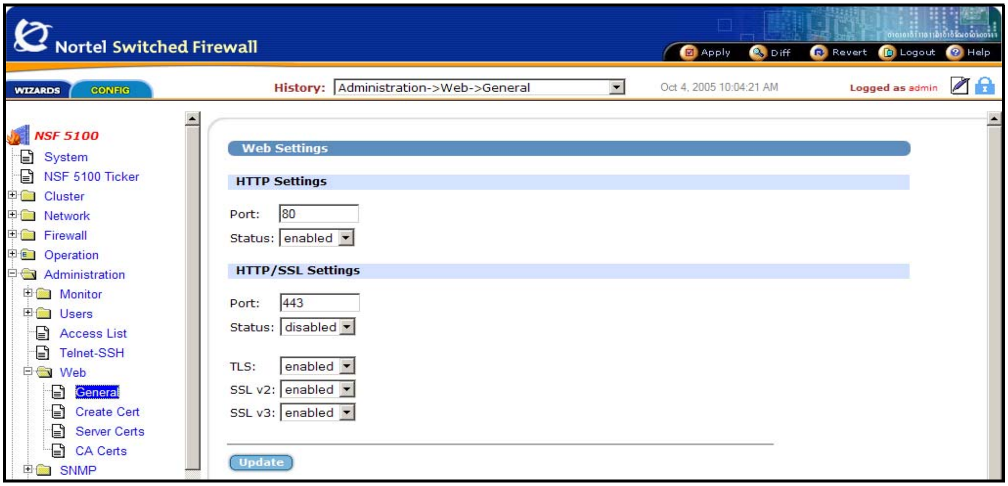
The four main categories of Administration/Web forms are:

- General (see Administration/Web/General form)
- Create Cert (see Administration/Web/Create Cert form on page 120)
- Server Certs (see Administration/Web/Server Certs form on page 121)
- CA Certs (see Administration/Web/CA Certs form on page 124)

Administration/Web/General form

The Administration/Web/General form enables web administration (see Administration/Web/General form).

Figure 86 Administration/Web/General form



History: Administration->Web->General

Oct 4, 2005 10:04:21 AM

Logged as admin

Web Settings

HTTP Settings

Port: 80

Status: enabled

HTTP/SSL Settings

Port: 443

Status: disabled

TLS: enabled

SSL v2: enabled

SSL v3: enabled

The Administration/Web/General form is divided into the following two sections for web settings:

- HTTP Settings
- HTTP/SSL Settings

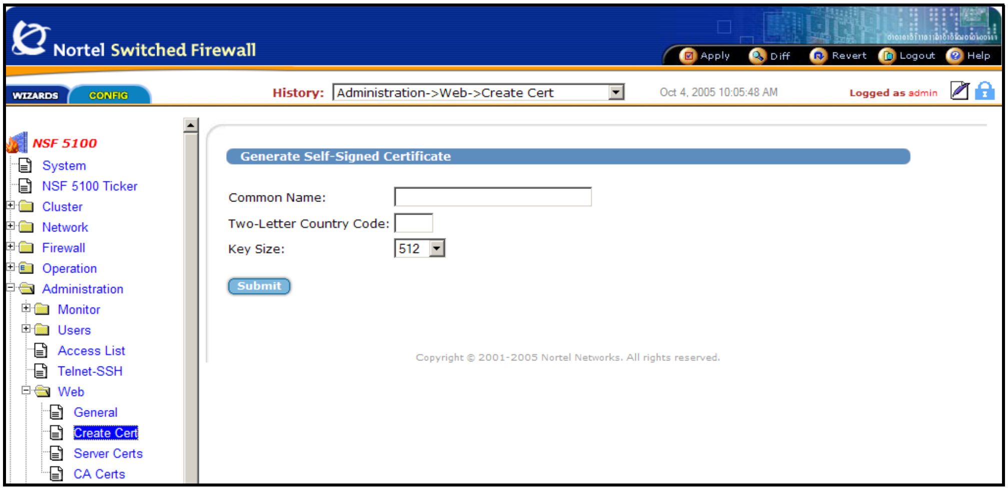
Fields and buttons on the form are as follows:

- HTTP Settings
  - □ Port provides an entry field to specify the port number for non-secure HTTP access to the BBI. **TIP**: The default is port 80.
  - □ Status provides a list with two selections:
    - o Enabled enables HTTP web administration.
    - o Disabled disables HTTP web administration.
- HTTP/SSL Settings
  - □ Port provides an entry field to specify the port number for SSL (secure HTTP) web administration.
  - □ Status provides a list with two selections:
    - o Enabled enables SSL web administration.
    - o Disabled disables SSL web administration.
  - □ TLS provides a list with two selections:
    - o Enabled enables TLS protocol.
    - o Disabled disables TLS protocol.
  - □ SSL v2 provides a list with two selections:
    - o Enabled enables SSL v2 protocol.
    - o Disabled disables SSL v2 protocol.
  - □ SSL v3 provides a list with two selections:
    - o Enabled enables SSL v3 protocol.
    - o Disabled disables SSL v3 protocol.
  - □ Update submits the web changes to the pending configuration.

Administration/Web/Create Cert form

The Administration/Web/Create Cert form provides a quick method to create a self-signed certificate that allows the BBI to run under SSL (see Administration/Web/Create Cert form). **TIP**: When the BBI is launched with HTTPS using this method, users can expect warnings from the web browser that the Certificate Authority (CA) root certificate is not trusted.

Figure 87 Administration/Web/Create Cert form



History: Administration->Web->Create Cert

Oct 4, 2005 10:05:48 AM

Logged as admin

Common Name:

Two-Letter Country Code:

Key Size: 512

Copyright © 2001-2005 Nortel Networks. All rights reserved.

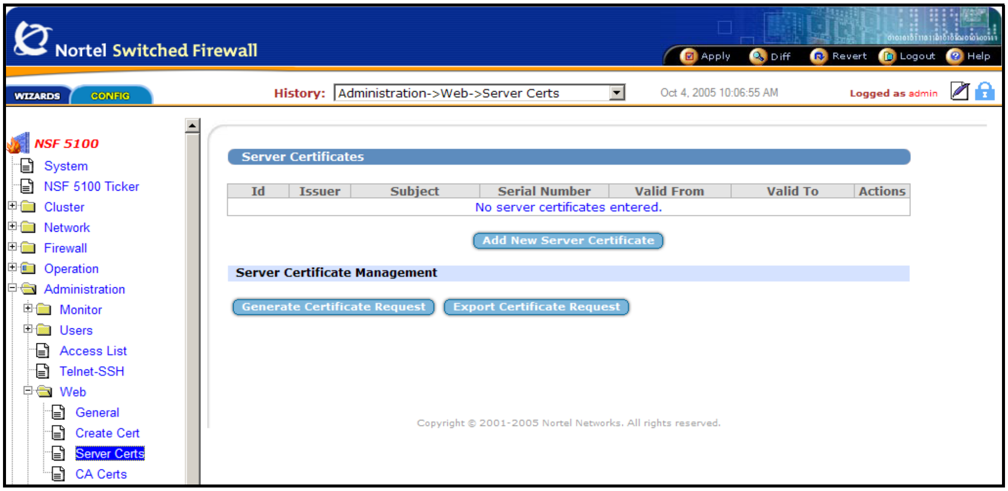
Fields and buttons on the Administration/Web/Create Cert form are as follows:

- Common Name provides an entry field to specify the common name for use with the certificate.
- Two-Letter Country Code provides an entry field to specify the country code to be used.
- Key Size provides a list to select the size of the encryption key with these selections:
  - 512
  - 1024
  - 2048
- Submit submits the self-signed certificate data to the pending configuration.

Administration/Web/Server Certs form

Use the Administration/Web/Server Certs form to administer server certificates on the Firewall (see Administration/Web/Server Certs form).

Figure 88 Administration/Web/Server Certs form



History: Administration->Web->Server Certs

Oct 4, 2005 10:06:55 AM

Logged as admin

Server Certificates

Id	Issuer	Subject	Serial Number	Valid From	Valid To	Actions
No server certificates entered.						

Server Certificate Management

Copyright © 2001-2005 Nortel Networks. All rights reserved.

The Administration/Web/Server Certs form is divided into the following two sections:

- Server Certificates
- Server Certificate Management

Fields and buttons on the form are as follows:

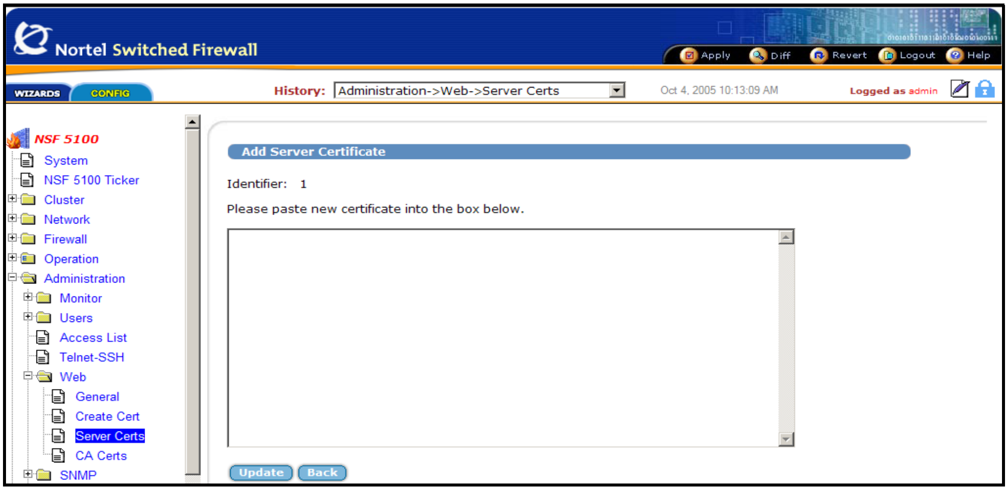
- Server Certificates
  - □ Id provides the identifier for the certificate.
  - □ Issuer identifies the issuer of the certificate.
  - □ Subject provides the subject of the certificate.
  - □ Serial Number provides the serial number of the certificate.
  - □ Valid From provides the date the certificate becomes valid.
  - □ Valid To provides the date the certificate expires.
  - □ Actions provides the following two selections visible if a certificate is present:
    - o Delete is used to delete a certificate from the system.
    - o Modify is used to modify the selected certificate.

  - Add New Server Certificate opens a form to add a new server certificate (see Administration/Web/Server Certs Add Server Certificate form).
- Server Certificate Management
  - Generate Certificate Request opens the request form (see Administration/Web/Server Certs/Generate Certificate Request form on page 123).
  - Export Certificate Request exports the certificate request.

Administration/Web/Server Certs Add Server Certificate form

Use the Administration/Web/Server Certs Add Server Certificate form to add a server certificate.

Figure 89 Administration/Web/Server Certs Add Server Certificate form



Add Server Certificate

Identifier: 1

Please paste new certificate into the box below.

Fields and buttons on the Administration/Web/Server Certs Add Server Certificate form are as follows:

- Identifier provides the assigned number of the certificate issuer.
- Update submits the certificate information to the pending configuration.
- Back returns to the Administration/Web/Server Certs page without submitting changes to the pending configuration.

Administration/Web/Server Certs/Generate Certificate Request form

Use the Administration/Web/Server Certs/Generate Certificate Request form to generate a certificate request (see Administration/Web/Server Certs/Generate Certificate Request form).

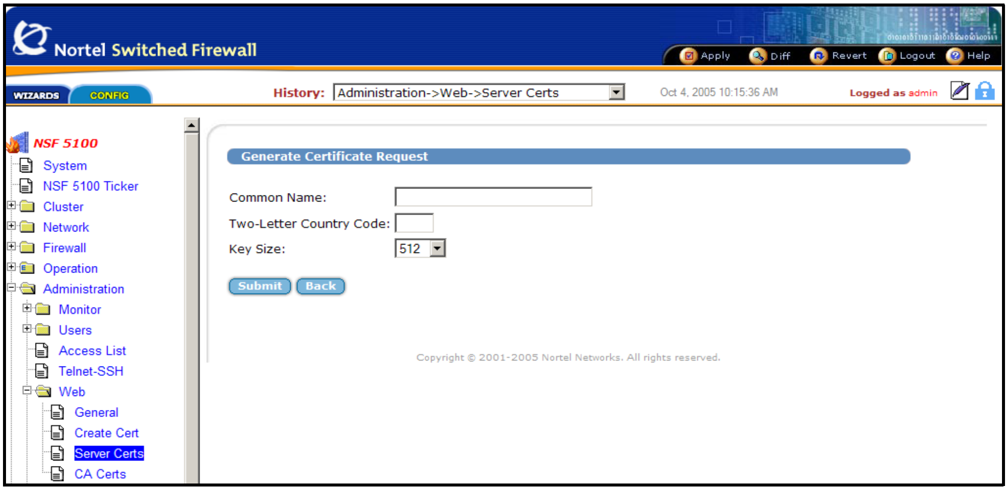


Figure 90 Administration/Web/Server Certs/Generate Certificate Request form

Generate Certificate Request

Common Name:

Two-Letter Country Code:

Key Size: 512

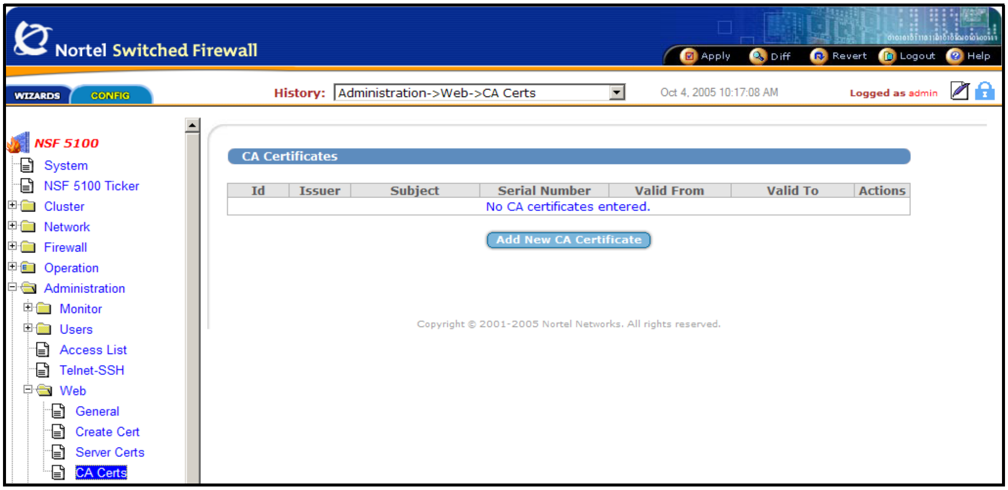
Fields and buttons on the Administration/Web/Server Certs Generate Certificate Request form are as follows:

- Common Name provides an entry field to specify the common name to be used with the certificate.
- Two-Letter Country Code provides an entry field to specify the country code.
- Key Size provides a list to specify the size, either 512, 1024, or 2048, of the encryption key.
- Submit submits the self-signed certificate data to the pending configuration.
- Back returns to the Administration/Web/Server Certs form without submitting changes to the pending configuration.

Administration/Web/CA Certs form

Use the Administration/Web/CA Certs form to administer Certificate Authority (CA) certificates on the Firewall (see Administration/Web/CA Certs form). CA certificates are required if server certificates from an external CA are used.

Figure 91 Administration/Web/CA Certs form



History: Administration->Web->CA Certs

Oct 4, 2005 10:17:08 AM

Logged as admin

CA Certificates

Id	Issuer	Subject	Serial Number	Valid From	Valid To	Actions
No CA certificates entered.						

Copyright © 2001-2005 Nortel Networks. All rights reserved.

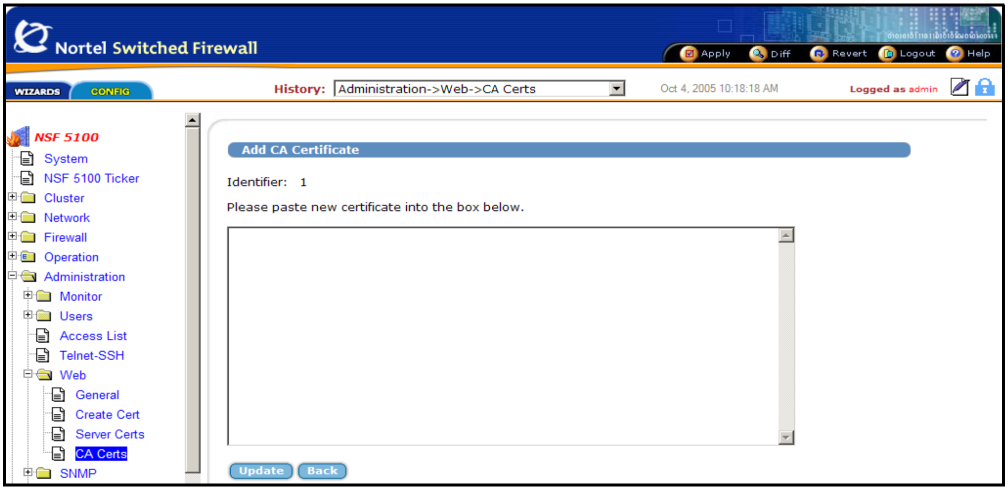
Fields and buttons on the Administration/Web/CA Certs form are as follows:

- Id provides an identifier for the certificate.
- Issuer identifies the issuer of the certificate.
- Subject provides the subject of the certificate.
- Serial Number provides the serial number for the certificate.
- Valid From provides the date the certificate becomes valid.
- Valid To provides the date the certificate expires.
- Actions provides the following two selections if a certificate is present:
  - Delete a certificate from the system.
  - Modify a selected certificate.
- Add New CA Certificate opens a form to add a new certificate (see Administration/Web/CA Certs Add Server Certificate form on page 125).

Administration/Web/CA Certs Add Server Certificate form

Use the Administration/Web/CA Certs Add Server Certificate form to add a server certificate.

Figure 92 Administration/Web/CA Certs Add Server Certificate form



Identifier: 1

Please paste new certificate into the box below.

Fields and buttons on the Administration/Web/CA Certs Add Server Certificate form are as follows:

- Identifier provides the assigned number of the certificate issuer.
- Update submits the certificate data to the pending configuration.
- Back returns to the Administration/Web/CA Certs form without submitting changes to the pending configuration.

SNMP forms

Use the Administration/SNMP forms to enable or disable SNMP event and alarm messages, enter administrative information for the SNMP system, list configured trap hosts, administer USM users, and configure the source IP address used with SNMP traps.

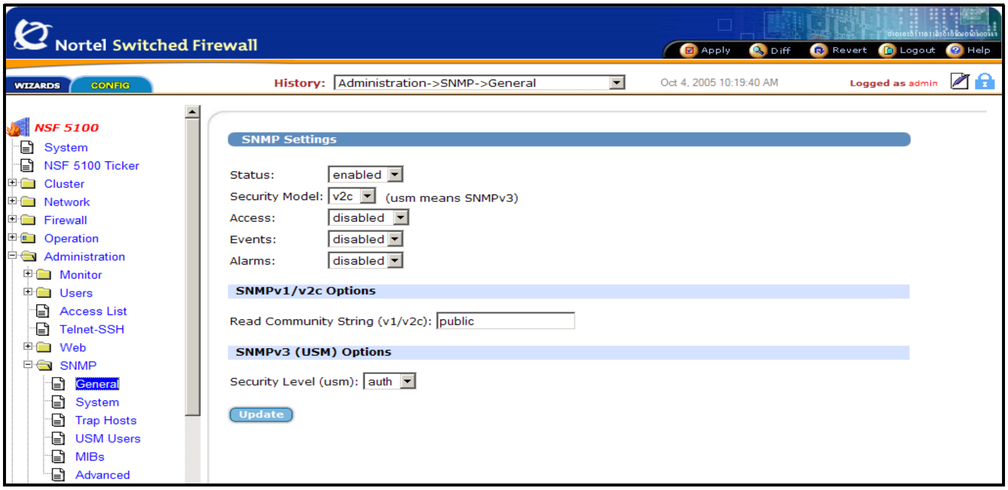
Administration/SNMP provides the following forms:

- General (see Administration/SNMP/General form)
- System (see Administration/SNMP/System form on page 128)
- Trap Hosts (see Administration/SNMP/Trap Hosts form on page 129)
- USM Users (see Administration/SNMP/USM Users form on page 131)
- MIBs (see Administration/SNMP/MIBs form on page 133)
- Advanced (see Administration/SNMP/Advanced form on page 134)

Administration/SNMP/General form

Use the Administration/SNMP/General form to enable or disable SNMP event and alarm messages for the Firewall (see Administration/SNMP/General form).

Figure 93 Administration/SNMP/General form



History: Administration->SNMP->General

Oct 4, 2005 10:19:40 AM

Logged as admin

SNMP Settings

Status: enabled

Security Model: v2c (usm means SNMPv3)

Access: disabled

Events: disabled

Alarms: disabled

SNMPv1/v2c Options

Read Community String (v1/v2c): public

SNMPv3 (USM) Options

Security Level (usm): auth

The Administration/SNMP/General form is divided into three sections:

- SNMP Settings
- SNMPv1/v2c Options

- SNMPv3 (USM) Options

Fields and buttons on the form are as follows:

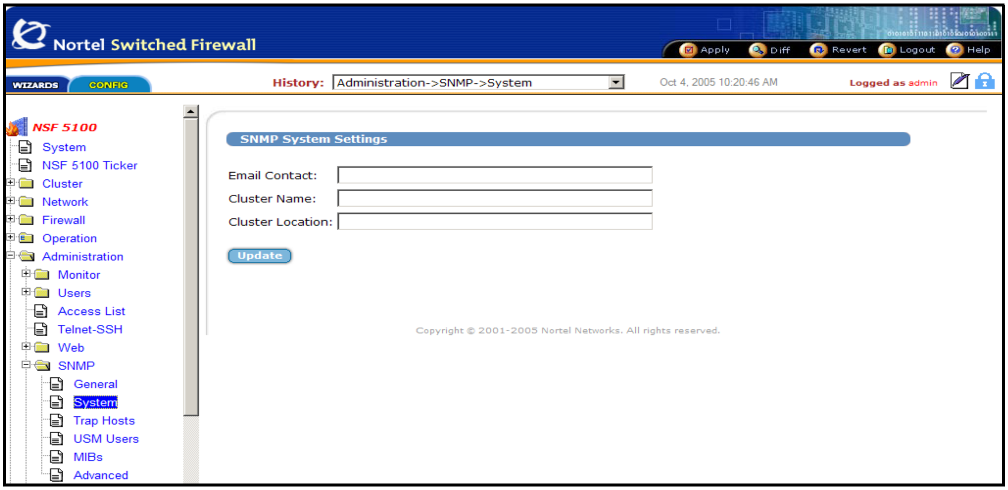
- SNMP Settings
  - Status provides a list with the following selections:
    - Enabled enables the SNMP agent.
    - Disabled disables the SNMP agent.
  - Security Model provides a list, used to specify the form of SNMP security, with the following selections:
    - v1 specifies the SNMPv1 security model.
    - v2c specifies the SNMPv2c security model.
    - usm specifies the SNMPv3 (USM) security model.
  - Access provides a list with the following selections:
    - Disabled disables SNMP read/write capacity. Users receive only enabled event and alarm messages.
    - Read permits read access.
    - Read/write permits read and write access.
  - Events provides a list with the following selections:
    - Enabled enables sending cluster event messages to SNMP trap hosts.
    - Disabled disables sending cluster event messages to SNMP trap hosts.
  - Alarms provides a list with the following selections:
    - Enabled enables sending cluster alarm messages to the SNMP trap hosts.
    - Disabled disables sending cluster alarm message to the SNMP trap hosts.
- SNMPv1/v2c Options
  - Read Community String (v1/v2c) default setting is public. **TIP**: Change the default for effective security.
- SNMPv3 (USM) Options
  - Security Level (usm)
    - none provides no authentication/privacy.
    - auth verifies the SNMP user before granting SNMP access and transmits in plain text.
      - priv verifies the SNMP user before granting SNMP access and transmits encrypted information.

□ Update submits the form changes to the pending configuration.

Administration/SNMP/System form

Use the Administration/SNMP/System form to enter administrative information on behalf of the SNMP system (see Administration/SNMP/System form).

Figure 94 Administration/SNMP/System form



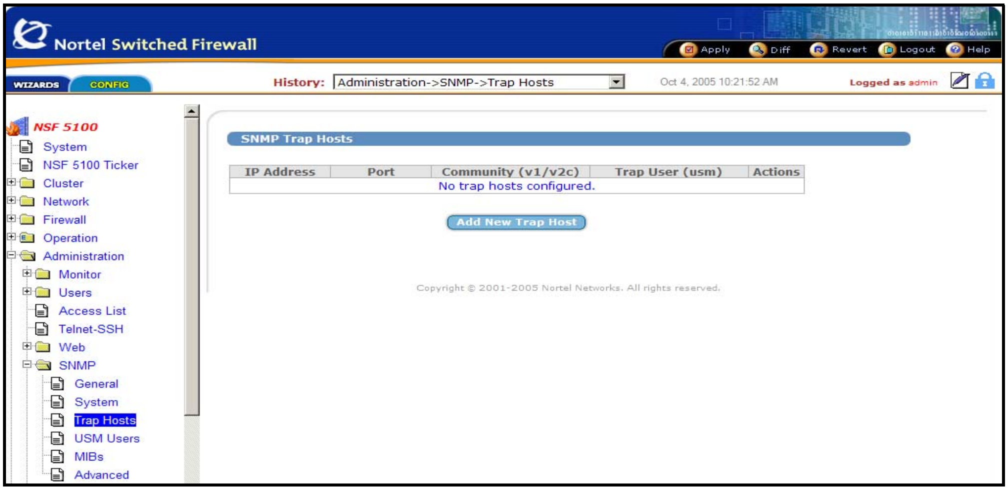
Fields and buttons on the Administration/SNMP/System form are as follows:

- Email Contact provides an entry field to specify the e-mail address of the SNMP administrator.
- Cluster Name provides an entry field to specify a name for referencing the cluster.
- Cluster Location provides an entry field to specify a name for referencing the cluster location.
- Update submits the form changes to the pending configuration.

Administration/SNMP/Trap Hosts form

The Administration/SNMP/Trap Hosts form lists configured trap hosts receiving SNMP event or alarm messages from the Firewall (see Administration/SNMP/Trap Hosts form).

Figure 95 Administration/SNMP/Trap Hosts form



History: Administration->SNMP->Trap Hosts

Oct 4, 2005 10:21:52 AM

Logged as admin

SNMP Trap Hosts

IP Address	Port	Community (v1/v2c)	Trap User (usm)	Actions
No trap hosts configured.				

Copyright © 2001-2005 Nortel Networks. All rights reserved.

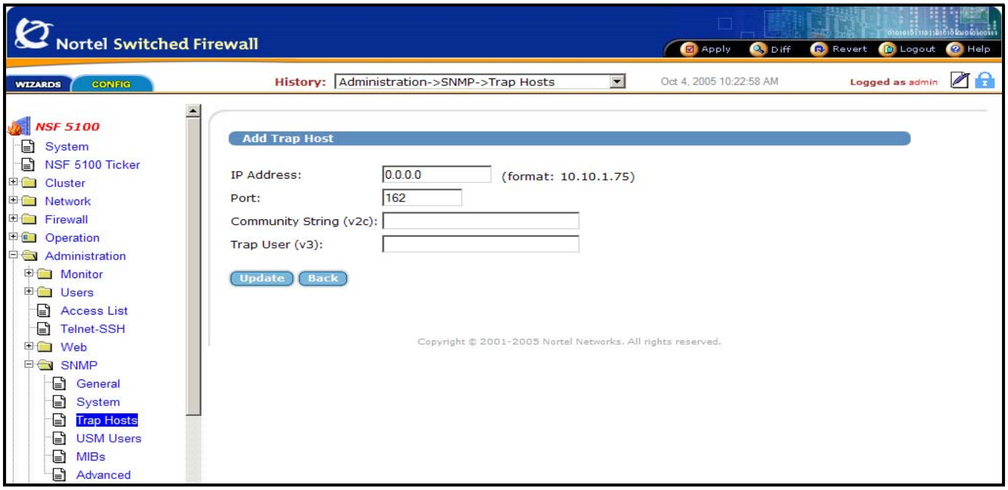
Fields and buttons on the Administration/SNMP/Trap Hosts form are as follows:

- IP Address specifies the IP address of the trap host. **TIP**: Use dotted decimal notation.
- Port specifies the destination port to which the trap should be sent. **TIP**: The default is port 162.
- Community (v1/v2c) specifies the community string for the trap host.
- Trap User (usm) specifies the user employed for trap authentication.
- Actions provides the following two options:
  - □ Delete deletes a trap host from the system.
  - □ Modify permits modification to the selected trap host.
- Add New Trap Host provides access to the add form (see Administration/SNMP/Trap Hosts Add Trap Host form on page 130).

Administration/SNMP/Trap Hosts Add Trap Host form

Use the Administration/SNMP/Trap Hosts Add Trap Host form to add a trap host.

Figure 96 Administration/SNMP/Trap Hosts Add Trap Host form



History: Administration->SNMP->Trap Hosts

Oct 4, 2005 10:22:58 AM

Logged as admin

Add Trap Host

IP Address:	0.0.0.0 (format: 10.10.1.75)
Port:	162
Community String (v2c):	
Trap User (v3):	

Copyright © 2001-2005 Nortel Networks. All rights reserved.

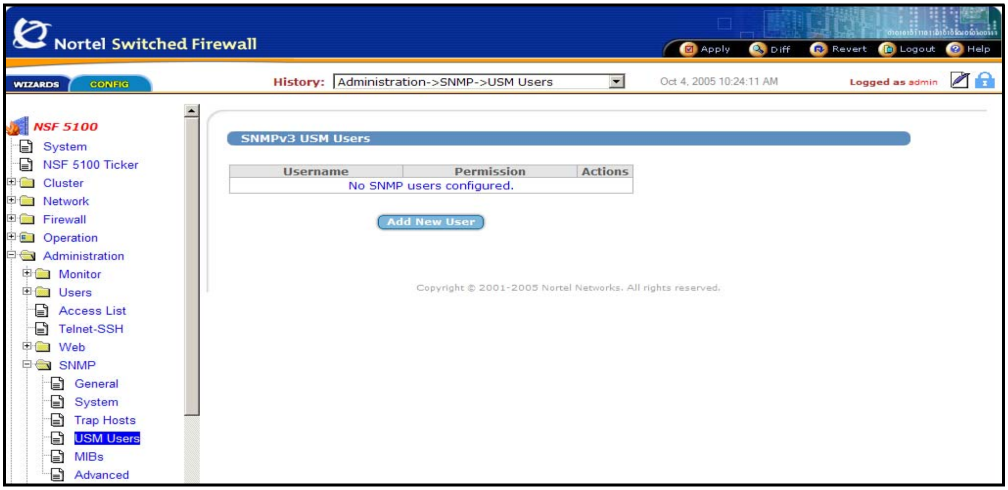
Fields and buttons on the Administration/SNMP/Trap Hosts Add Trap Host form are as follows:

- IP Address provides an entry field to specify the IP address of the trap host.
- Port provides an entry field to specify the port to send the trap. **TIP**: The SNMP default port is 162.
- Community String v2c provides an entry field to specify the community string for the trap host.
- Trap user (v3) provides an entry field to specify the user employed for trap authentication.
- Update submits new SNMP User Name information to the pending configuration.
- Back returns to the Administration/SNMP/Trap Hosts form without submitting changes to the pending configuration.

Administration/SNMP/USM Users form

Use the Administration/SNMP/USM Users form to administer USM users employed in SNMP v3 (usm) authentication and encryption (see Administration/SNMP/USM Users form).

Figure 97 Administration/SNMP/USM Users form



Username	Permission	Actions
No SNMP users configured.		

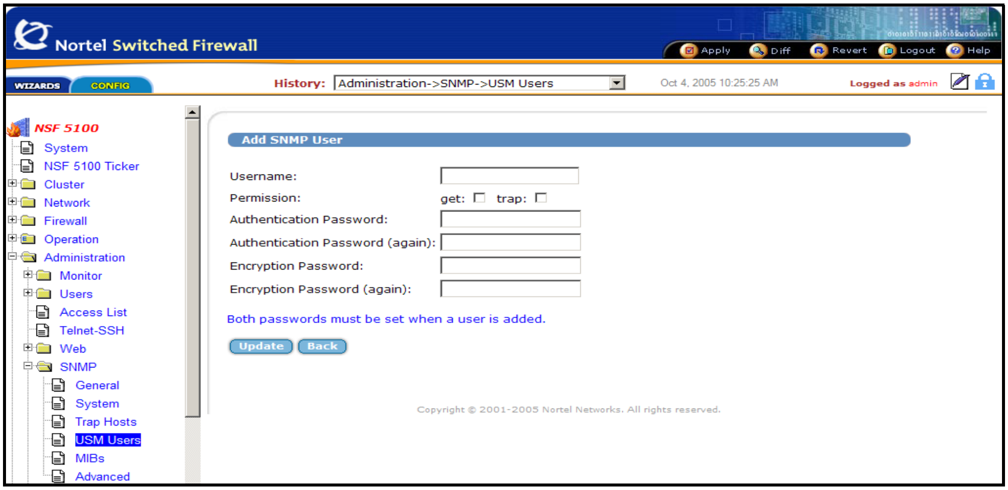
Fields and buttons on the Administration/SNMP/USM Users form are as follows:

- Username specifies the name of the user for SNMP v3 (usm) authentication and encryption.
- Permission specifies the user permission type: read, trap, or read/trap.
- Actions provides the following two selections:
  - Delete deletes a user from the system.
  - Modify permits modification of the selected user parameters.
- Add New User opens the Add SNMP User form (see Administration/SNMP/USM Users Add SNMP User form on page 132).

Administration/SNMP/USM Users Add SNMP User form

Use the Administration/SNMP/USM Users Add SNMP User form to add a new SNMP user.

Figure 98 Administration/SNMP/USM Users Add SNMP User form



History: Administration->SNMP->USM Users

Oct 4, 2005 10:25:25 AM

Add SNMP User

Username:	
Permission:	get: □ trap: □
Authentication Password:	
Authentication Password (again):	
Encryption Password:	
Encryption Password (again):	

Both passwords must be set when a user is added.

Copyright © 2001-2005 Nortel Networks. All rights reserved.

Fields and buttons on the Administration/SNMP/USM Users Add SNMP User form are as follows:

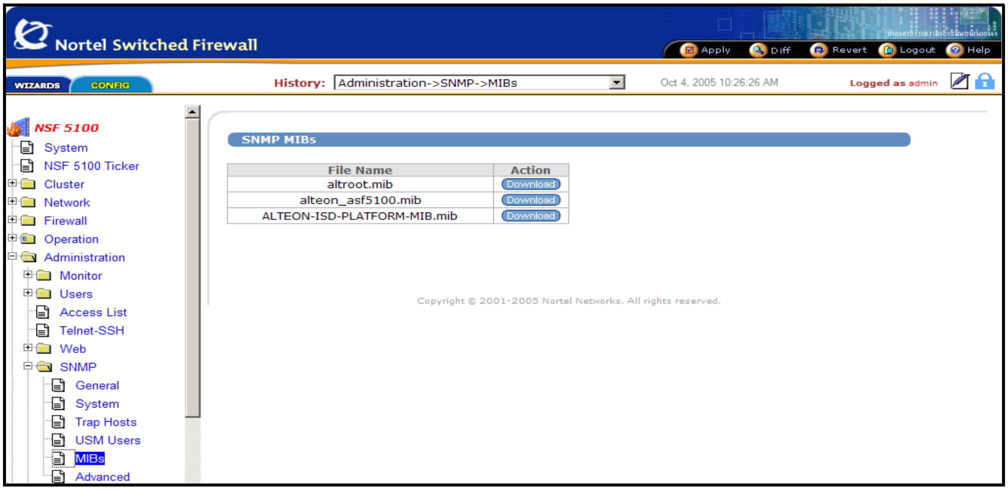
- Username provides an entry field to specify the name of the user for SNMP v3 (usm) authentication/encryption.
- Permission provides two check boxes to specify the type of permission allowed for the user:
  - Get
  - Trap
- Authentication Password provides an entry field to specify the password used in MD5 authentication.
- Authentication Password (again) provides an entry field to confirm the password.
- Encryption Password provides an entry field to specify the password used in DES entryption.
- Encryption Password (again) provides an entry field to confirm the password. **TIP**: When a user is added, set both passwords.
- Update submits the new trap host data to the pending configuration.

- Back returns to the Administration/SNMP/USM/Users form without submitting changes to the pending configuration.

Administration/SNMP/MIBs form

The Administration/SNMP/MIBs form displays all of the SNMP MIB files available on the Firewall (see Administration/SNMP/MIBs form).

Figure 99 Administration/SNMP/MIBs form



History: Administration->SNMP->MIBs

SNMP MIBs

File Name	Action
altroot.mib	Download
alteon_asf5100.mib	Download
ALTEON-ISD-PLATFORM-MIB.mib	Download

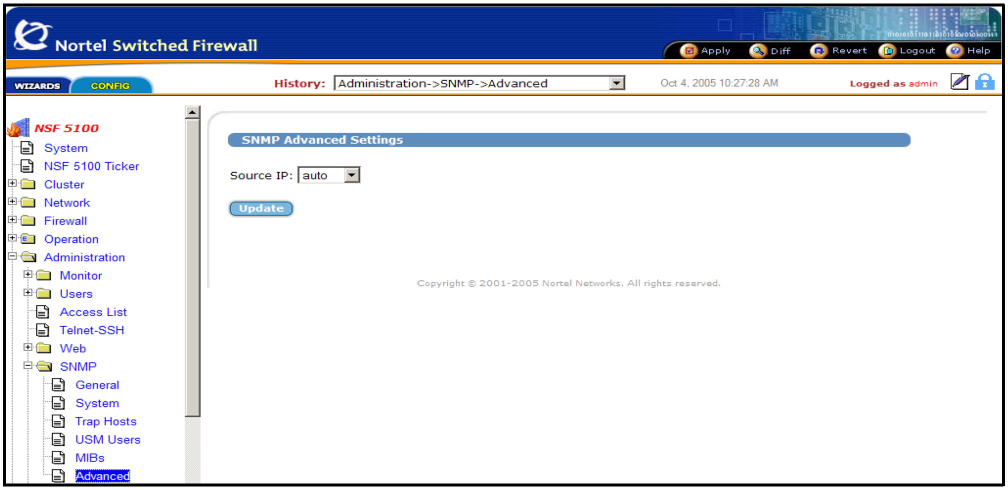
Fields and buttons on the Administration/SNMP/MIBs form are as follows:

- File Name lists the SNMP MIB files existing on the Firewall.
- Action
  - Download permits downloading of the selected MIB file to the client system.

Administration/SNMP/Advanced form

Use the Administration/SNMP/Advanced form to configure the source IP address used with SNMP traps generated from the Firewall (see Administration/SNMP/Advanced form).

Figure 100 Administration/SNMP/Advanced form



History: Administration->SNMP->Advanced

Oct 4, 2005 10:27:28 AM

Source IP: auto

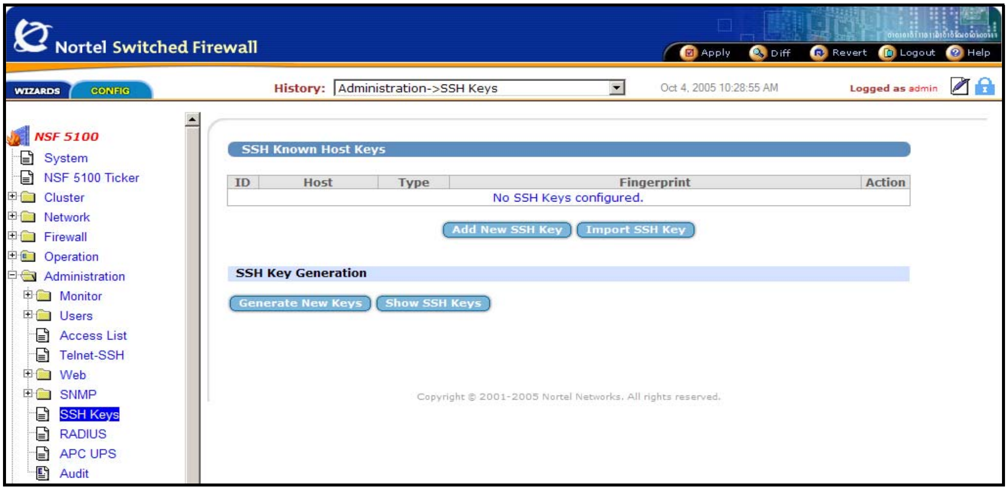
Fields and buttons on the Administration/SNMP/Advanced form are as follows:

- Source IP provides a list with the following selections:
  - auto is the default and uses the IP address of the outgoing interface.
  - unique uses the IP address of the NSF management port.
  - MIP uses the cluster MIP address.
- Update submits the source IP information to the pending configuration.

SSH Keys form

Use the Administration/SSH keys form to display the current Host Keys and generate new SSH keys for the cluster (see Administration/SSH keys form).

Figure 101 Administration/SSH keys form



History: Administration->SSH Keys

Oct 4, 2005 10:28:55 AM

Logged as admin

SSH Known Host Keys

ID	Host	Type	Fingerprint	Action
			No SSH Keys configured.	

SSH Key Generation

Copyright © 2001-2005 Nortel Networks. All rights reserved.

The Administration/SSH keys form is divided into the following two sections:

- SSH Known Host Keys
- SSH Key Generation

Fields and buttons on the Administration/SSH keys form are as follows:

- SSH Known Host Keys displays the current host keys for the cluster. This section is used to manage known SSH host keys of firewalls and includes the following fields and buttons:
  - ID is the numerical ID of the generated SSH key.
  - Host is the IP address of the remote host containing the SSH key import target.
  - Type specifies the encryption type of the SSH key—RSA or DES.
  - Fingerprint displays the fingerprint of the SSH key.
  - Action provides a Delete button if SSH keys are configured. Click **Delete** to delete the specific SSH key from the registry.
  - Add New SSH Key formats and stores the specified SSH key (see Administration/SSH keys Add New SSH key form on page 136).

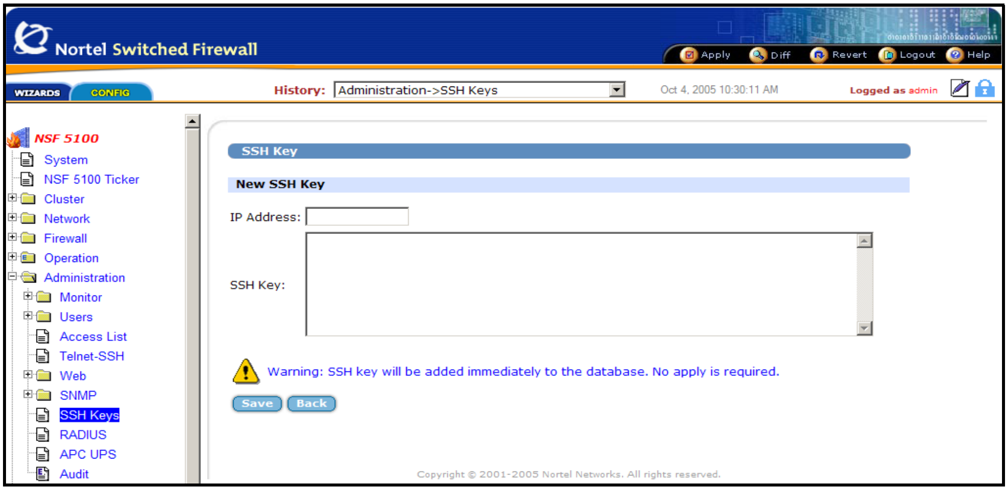
  - □ Import SSH Key imports an SSH key from a remote host (see Administration/SSH Keys Import SSH Key form on page 137).

- SSH Key Generation includes the following fields and buttons:
  - □ Generate new Keys generates new SSH keys.
  - □ Show SSH Keys shows the current SSH host keys for the cluster (see Administration/SSH Keys Show SSH keys form on page 138).

Administration/SSH keys Add New SSH key form

Use the Administration/SSH keys Add New SSH key form to add SSH keys to the configuration.

Figure 102 Administration/SSH keys Add New SSH key form



History: Administration->SSH Keys

Oct 4, 2005 10:30:11 AM

Logged as admin

IP Address:

SSH Key:

Warning: SSH key will be added immediately to the database. No apply is required.

Copyright © 2001-2005 Nortel Networks. All rights reserved.

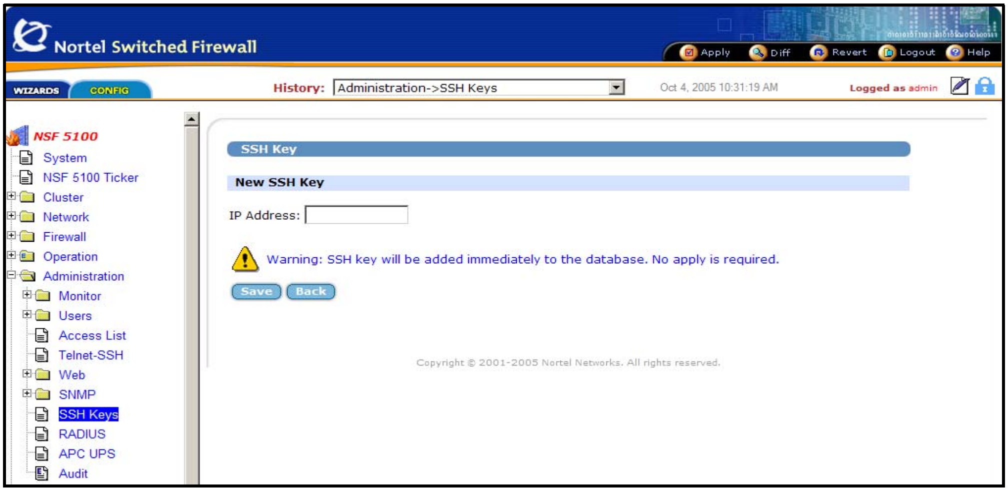
Fields and buttons on the Administration/SSH keys Add New SSH key form are as follows:

- IP Address provides an entry field to specify the IP address of the firewall.
- SSH Key displays the SSH host keys of the specified firewall.
- Save applies the changes without sending them to the pending configuration.
- Back returns to the Administration/SSH keys for without submitting changes to the pending configuration.

Administration/SSH Keys Import SSH key form

Use the Administration/SSH Keys Import SSH Key form to import SSH keys (see Administration/SSH Keys Import SSH Key form).

Figure 103 Administration/SSH Keys Import SSH Key form



History: Administration->SSH Keys

Oct 4, 2005 10:31:19 AM

Logged as admin

SSH Key

New SSH Key

IP Address:

Warning: SSH key will be added immediately to the database. No apply is required.

Copyright © 2001-2005 Nortel Networks. All rights reserved.

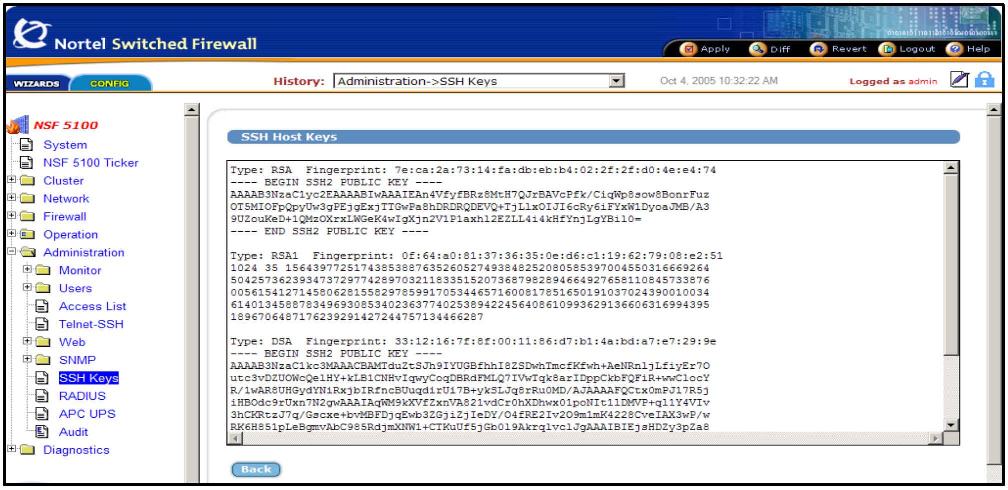
Fields and buttons on the Administration/SSH Keys Import SSH Key form are as follows:

- IP Address provides an entry field to specify the IP address of the Firewall.
- Click **Save** to apply the changes without sending them to the pending configuration.
- Click **Back** to return to the Administration/SSH Keys form without submitting changes to the pending configuration.

Administration/SSH Keys Show SSH keys form

Use the Administration/SSH Keys Show SSH keys form to view resident SSH key information (see Administration/SSH Keys Show SSH keys form).

Figure 104 Administration/SSH Keys Show SSH keys form



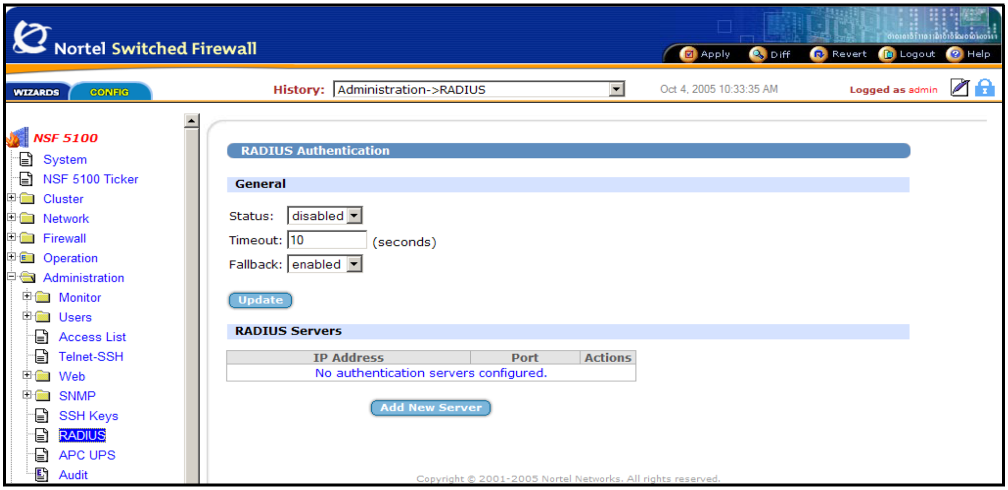
```
Type: RSA  Fingerprint: 7e:ca:2a:73:14:fa:db:eb:b4:02:2f:2f:d0:4e:e4:74
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAABIwAAAIEAn4VfyfBRz8MtH7QJrBAVcPfk/CiqWp8sow8BonrFuz
OT5MIOFpQpyUw3gPEjgExjTTGwPa8hDRDRQDEVQ+TjLlxOIJI6cRy6iFYxW1DyoaJMB/A3
9UZouKeD+1QMzOXrxLWGeK4wIgXjn2V1P1axhl2EZLL4i4kHfYnjLgYBil0=
---- END SSH2 PUBLIC KEY ----

Type: RSA1  Fingerprint: 0f:64:a0:81:37:36:35:0e:d6:c1:19:62:79:08:e2:51
1024 35 15643977251743853887635260527493848252080585397004550316669264
5042573623934737297742897032118335152073687982894664927658110845733876
0056154127145806281558297859917053446571600817851650191037024390010034
6140134588783496930853402363774025389422456408610993629136606316994395
18967064871762392914272444757134466287

Type: DSA  Fingerprint: 33:12:16:7f:8f:00:11:86:d7:b1:4a:bd:a7:e7:29:9e
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1kc3MAAACBAMTduZtSJh9IYUGBfhhI8ZSDwhTmcfKfwh+AeNRnljLfiyEr7O
utc3vDZUOWcQelHY+kLB1CNHvIqwyCoqDBRdFMLQ7IVwTqk8arIDppCkbFQFiR+wwClocY
R/1wAR8UHGydYNiRxjbIRfncBUuqdirUi7B+ykSLJq8rRu0MD/AJAAAAFQCtx0mPJ17R5j
iHBOdc9rUxn7N2gwAAAIAqWM9kXVfZxnVA821vdCr0hXDhwx01poNIt1lDMVP+ql1Y4VIv
3hCKRtzJ7q/Gscxe+bvMBFDjqEwb3ZGjiZjIeDY/O4fRE2Iv2O9m1mK4228CveIAX3wP/w
RK6H851pLeBgmvAbC985RdjmXNW1+CTKuUf5jGb0l9AkrqlvclJgAAAIBIEjsHDZy3pZa8
```

Click **Back** to return to the Administration/SSH keys form.

RADIUS form

Use the Administration/RADIUS form to configure RADIUS authentication for system users (see Administration/RADIUS form).

Figure 105 Administration/RADIUS form



General

Status: disabled

Timeout: 10 (seconds)

Fallback: enabled

RADIUS Servers

IP Address	Port	Actions
No authentication servers configured.		

The Administration/RADIUS form is divided into the following two sections:

- General
- RADIUS Servers

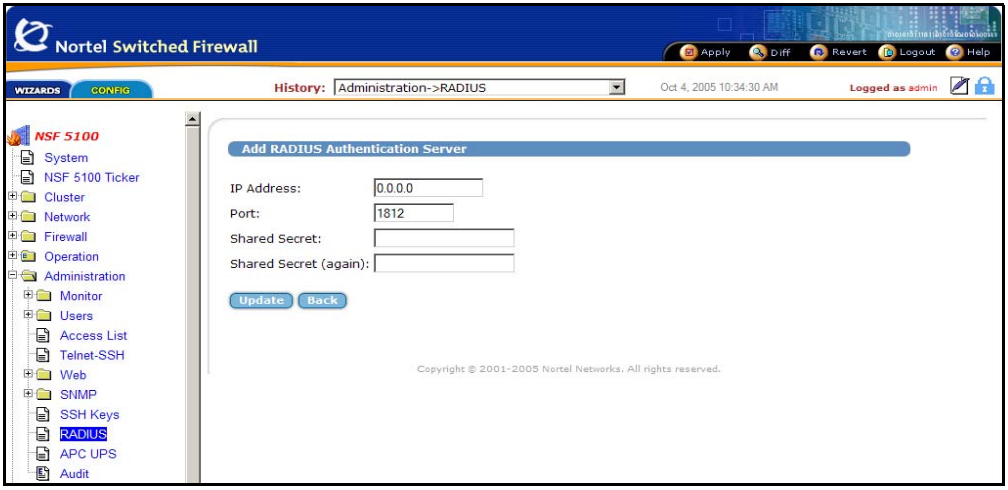
Fields and buttons on the form are as follows:

- General
  - Status provides a list with the following two selections:
    - Enabled enables RADIUS authentication of system users.
    - Disabled disables RADIUS authentication of system users. **TIP**: Disabled is the default setting.
  - Timeout provides an entry field to specify a timeout value, in seconds, for a connection request to a RADIUS server. **TIP**: The default timeout value is 10 seconds.
  - Fallback specifies the desired fallback mode and provides a list with the following two selections:
    - Enabled specifies that local passwords are used as fallback if the RADIUS servers are unreachable. **TIP**: Enabled is the default parameter.
    - Disabled fallback mode specifies that local passwords cannot be used as fallback if the RADIUS servers are unreachable.
  - Update submits the settings to the pending configuration.
- RADIUS Servers
  - IP Address specifies the IP address of the RADIUS server.
  - Port specifies the TCP port of the RADIUS server.
  - Actions
    - Modify provides a form for modifying the selected RADIUS server.
    - Delete deletes the selected RADIUS server.
  - Add New Server provides a form for adding a new RADIUS server (see Administration/RADIUS Add RADIUS Authentication Server form on page 140).

Administration/RADIUS Add RADIUS Authentication Server form

Use the Administration/RADIUS Add RADIUS Authentication Server form to add a RADIUS Authentication server.

Figure 106 Administration/RADIUS Add RADIUS Authentication Server form



History: Administration->RADIUS

Oct 4, 2005 10:34:30 AM

Logged as admin

Add RADIUS Authentication Server

IP Address:	0.0.0.0
Port:	1812
Shared Secret:	
Shared Secret (again):	

Copyright © 2001-2005 Nortel Networks. All rights reserved.

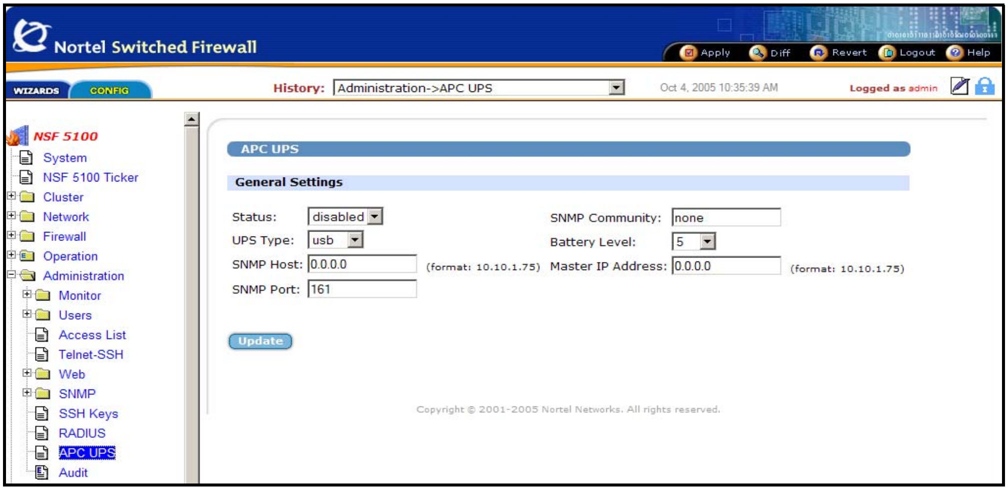
Fields and buttons on the Administration/RADIUS Add RADIUS Authentication Server form are as follows:

- IP Address provides an entry field to specify the IP address of the RADIUS server.
- Port provides an entry field to specify the TCP port of the RADIUS server.
- Shared Secret provides an entry field to specify the shared secret used by the RADIUS server.
- Shared Secret (again) provides an entry field to confirm the Shared Secret.
- Update submits the changes to the pending configuration.
- Back returns to the Administration/RADIUS page without submitting changes to the pending configuration.

APC UPS form

Use the Administration/APC UPS form to configure settings for American Power Corporation Uninterrupted Power Supply (APC UPS) (see Administration/APC UPS form).

Figure 107 Administration/APC UPS form



Status: disabled

UPS Type: usb

SNMP Host: 0.0.0.0 (format: 10.10.1.75)

SNMP Port: 161

SNMP Community: none

Battery Level: 5

Master IP Address: 0.0.0.0 (format: 10.10.1.75)

Fields and buttons on the Administration/APC/UPS form are as follows:

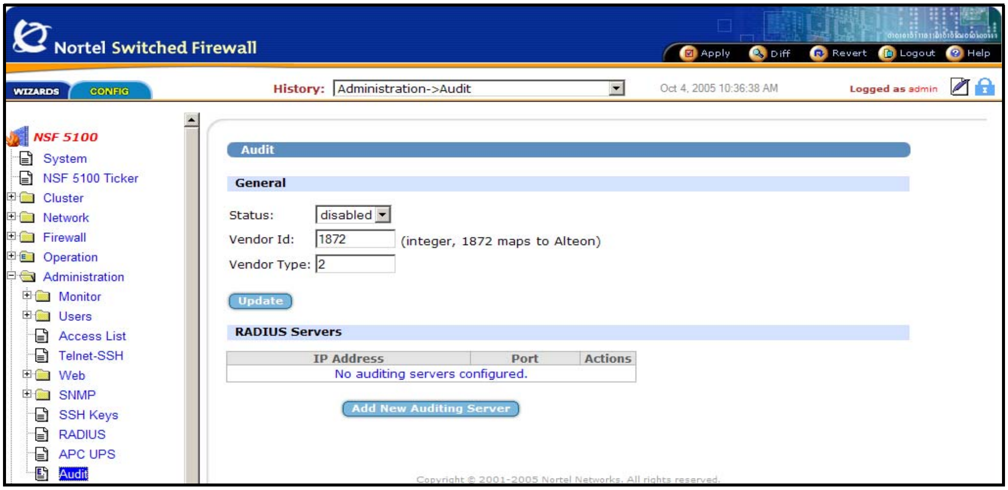
- Status provides a list with the following two selections:
  - Enabled enables the UPS monitor.
  - Disabled disables the UPS monitor.
- UPS Type provides a list to set the UPS type from the following selections:
  - usb (USB port)
  - snmp (Ethernet through SNMP)
- SNMP Host provides an entry field to specify the SNMP Host IP address for connection. **TIP**: Use dotted decimal notation.
- SNMP Port provides an entry field to specify the SNMP port for connection.
- SNMP Community provides an entry field to set the SNMP community for connection.
- Battery Level provides a list to specify the battery level, in percentage, below which the Firewall shuts down. The list represents a range from 0 to 100 percent.
- Master IP Address provides an entry field to specify the UPS Master IP address. **TIP**: Use dotted decimal notation.

- Update submits the UPS Monitor changes to the pending configuration.

Audit form

Use the Administration/Audit form to configure a RADIUS server to receive log messages about commands executed in the CLI (see Administration/Audit form).

Figure 108 Administration/Audit form



History: Administration->Audit

Audit

General

Status: disabled

Vendor Id: 1872 (integer, 1872 maps to Alteon)

Vendor Type: 2

RADIUS Servers

IP Address	Port	Actions
No auditing servers configured.		

The Administration/Audit form is divided into the following two sections:

- General
- RADIUS Servers

Fields and buttons on the form are as follows:

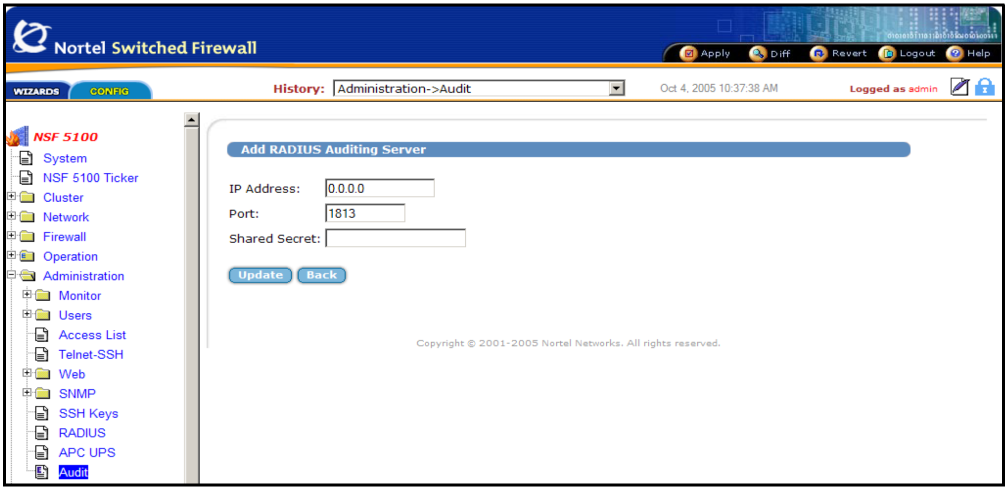
- General
  - □ Status provides a list with the following selections:
    - o Enabled permits the CLI login, logout, and update events to be sent to the event log, any configured syslog servers, and to a RADIUS audit server.
    - o Disabled disables auditing.
  - □ Vendor Id provides an entry field to specify the SMI Network Management Private Enterprise Code. **TIP**: The default is 1872, Alteon (NSF).
  - □ Vendor Type provides an entry field to specify a number representing the vendor type attribute used in RADIUS. **TIP**: The default vendor type value is 2.
  - □ Update submits the changes to the pending configuration.

- RADIUS Servers
  - □ IP Address provides the address of a configured RADIUS server or an entry field to change or specify the IP Address of a RADIUS server.
  - □ Port provides the TCP port number or an entry field to change or specify the TCP port number.
  - □ Actions provides the following two options:
    - o Delete deletes a selected RADIUS server.
    - o Modify opens a form to modify the selected RADIUS server settings.
  - □ Add New Auditing Server (see Administration/Audit Add RADIUS Auditing Server form)

Administration/Audit Add RADIUS Auditing Server form

Use the Administration/Audit Add RADIUS Auditing Server form to add a RADIUS auditing server.

Figure 109 Administration/Audit Add RADIUS Auditing Server form



Add RADIUS Auditing Server

IP Address: 0.0.0.0

Port: 1813

Shared Secret:

Fields and buttons on the Administration/Audit Add RADIUS Auditing Server form are as follows:

- IP Address provides an entry field to specify the IP address of the RADIUS auditing server.
- Port provides and entry field to specify the TCP port number.
- Shared secret provides an entry field to specify the RADIUS shared secret.

- Update submits the changes to the pending configuration.
- Back returns to the Administration/Audit form without submitting changes to the pending configuration.

Diagnostics forms

The Diagnostics forms provide information about logs, forms to check configuration and Check Point Logs, system commands, and OSPF Debug settings.

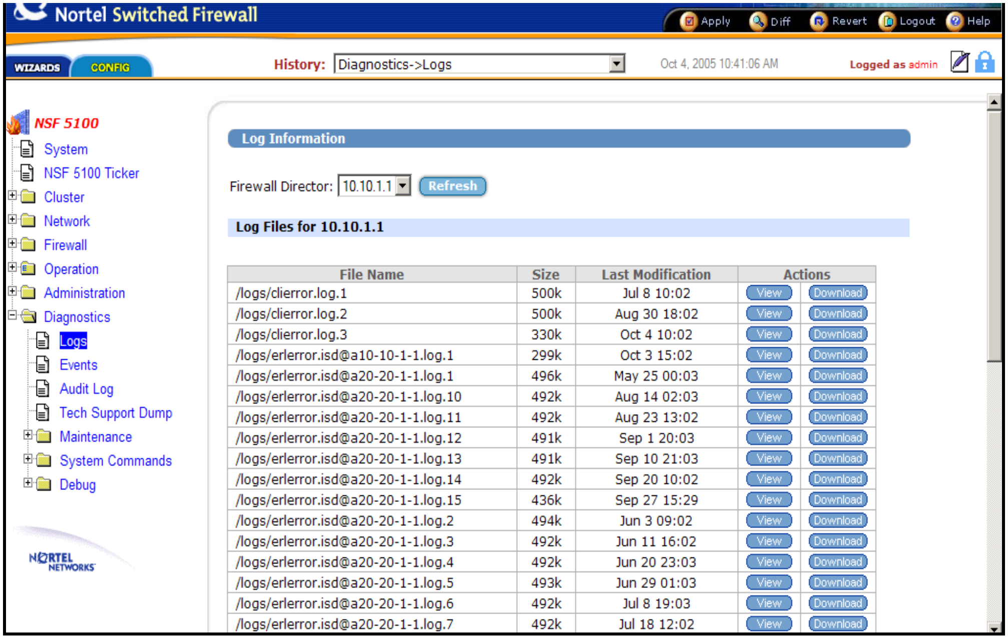
The Diagnostic forms menu includes the following categories of forms:

- Logs (see Logs form)
- Events (see Events form on page 147)
- Audit Log (see Audit Log form on page 148)
- Maintenance (see Maintenance forms on page 149)
- System Commands (see System Commands form on page 151)
- Debug (see Debug forms on page 152)

Logs form

The Diagnostics/Logs form displays the contents of the log file collected from the selected Firewall host (see Diagnostics/Logs form).

Figure 110 Diagnostics/Logs form



History: Diagnostics->Logs

Oct 4, 2005 10:41:06 AM

Logged as admin

Log Information

Firewall Director: 10.10.1.1 Refresh

Log Files for 10.10.1.1

File Name	Size	Last Modification	Actions	
/logs/clierror.log.1	500k	Jul 8 10:02	View	Download
/logs/clierror.log.2	500k	Aug 30 18:02	View	Download
/logs/clierror.log.3	330k	Oct 4 10:02	View	Download
/logs/erlerror.isd@a10-10-1-1.log.1	299k	Oct 3 15:02	View	Download
/logs/erlerror.isd@a20-20-1-1.log.1	496k	May 25 00:03	View	Download
/logs/erlerror.isd@a20-20-1-1.log.10	492k	Aug 14 02:03	View	Download
/logs/erlerror.isd@a20-20-1-1.log.11	492k	Aug 23 13:02	View	Download
/logs/erlerror.isd@a20-20-1-1.log.12	491k	Sep 1 20:03	View	Download
/logs/erlerror.isd@a20-20-1-1.log.13	491k	Sep 10 21:03	View	Download
/logs/erlerror.isd@a20-20-1-1.log.14	492k	Sep 20 10:02	View	Download
/logs/erlerror.isd@a20-20-1-1.log.15	436k	Sep 27 15:29	View	Download
/logs/erlerror.isd@a20-20-1-1.log.2	494k	Jun 3 09:02	View	Download
/logs/erlerror.isd@a20-20-1-1.log.3	492k	Jun 11 16:02	View	Download
/logs/erlerror.isd@a20-20-1-1.log.4	492k	Jun 20 23:03	View	Download
/logs/erlerror.isd@a20-20-1-1.log.5	493k	Jun 29 01:03	View	Download
/logs/erlerror.isd@a20-20-1-1.log.6	492k	Jul 8 19:03	View	Download
/logs/erlerror.isd@a20-20-1-1.log.7	492k	Jul 18 12:02	View	Download

The Diagnostics/Logs form is divided into the following two sections:

- Log Information
- Log Files

Fields and buttons on the form are as follows:

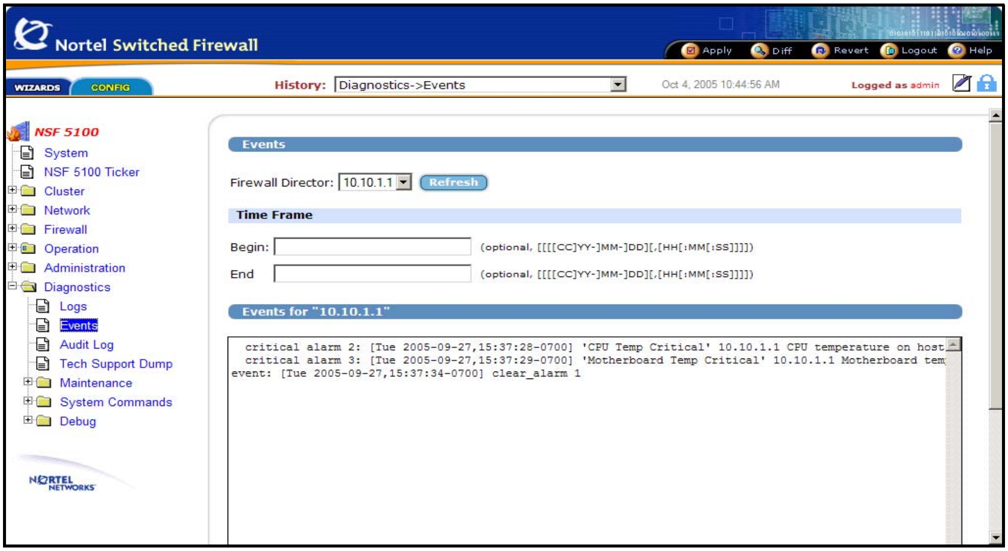
- Log Information
  - Firewall Director provides a list containing the IP addresses of the Firewall Directors.
    - Refresh displays the details of the selected Firewall Director.
- Log Files lists all of the log files on the selected Firewall.
  - File Name displays the names of log files.
  - Size displays the size of log files.
  - Last Modification provides the date or most recent modification of the log files.
  - Actions provides the following two selections:
    - View displays the contents of a selected log file.
    - Download downloads the contents of a selected log file to the local system.

NOTE – Only the most recent 64 K of log information is displayed.

Events form

The Diagnostics/Events form displays the contents of the event log file (see Diagnostics/Events form).

Figure 111 Diagnostics/Events form



History: Diagnostics->Events

Oct 4, 2005 10:44:56 AM

Logged as admin

Events

Firewall Director: 10.10.1.1

Time Frame

Begin: (optional, [[[[CC]YY-]MM-]DD][,[HH[:MM[:SS]]]])

End (optional, [[[[CC]YY-]MM-]DD][,[HH[:MM[:SS]]]])

Events for "10.10.1.1"

```
  critical alarm 2: [Tue 2005-09-27,15:37:28-0700] 'CPU Temp Critical' 10.10.1.1 CPU temperature on host
  critical alarm 3: [Tue 2005-09-27,15:37:29-0700] 'Motherboard Temp Critical' 10.10.1.1 Motherboard tem
event: [Tue 2005-09-27,15:37:34-0700] clear_alarm 1
```

Fields and buttons on the Diagnostics/Events form are as follows:

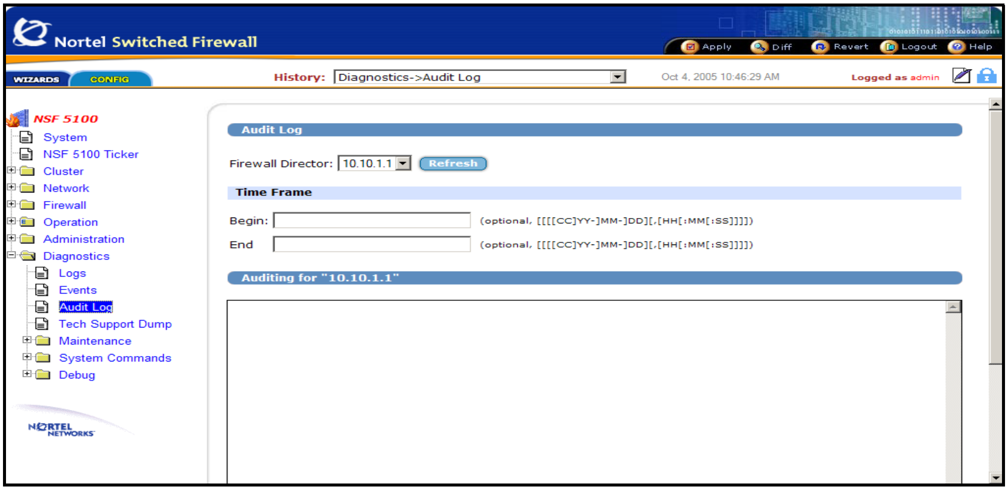
- Firewall Director provides a list containing the IP addresses of the Firewall Directors. Refresh displays the details of the selected Firewall Director.
- Time Frame provides two entry fields for setting the time filters for displaying event information.
  - Begin provides an entry field for setting the begin time filter.
  - End provides an entry field for setting the end time filter.
- Events displays the information extracted from the event log file on the selected Firewall Director.

NOTE – Only the most recent 64 K of event information is displayed.

Audit Log form

Use the Diagnostics/Audit Log form to display the latest 64 K of the device audit log (see Diagnostics/Audit Log form).

Figure 112 Diagnostics/Audit Log form



Firewall Director: 10.10.1.1

Begin: (optional, [[[[CC]YY-]MM-]DD][,[HH[:MM[:SS]]]])

End (optional, [[[[CC]YY-]MM-]DD][,[HH[:MM[:SS]]]])

Fields and buttons on the Diagnostic/Audit Log form are as follows:

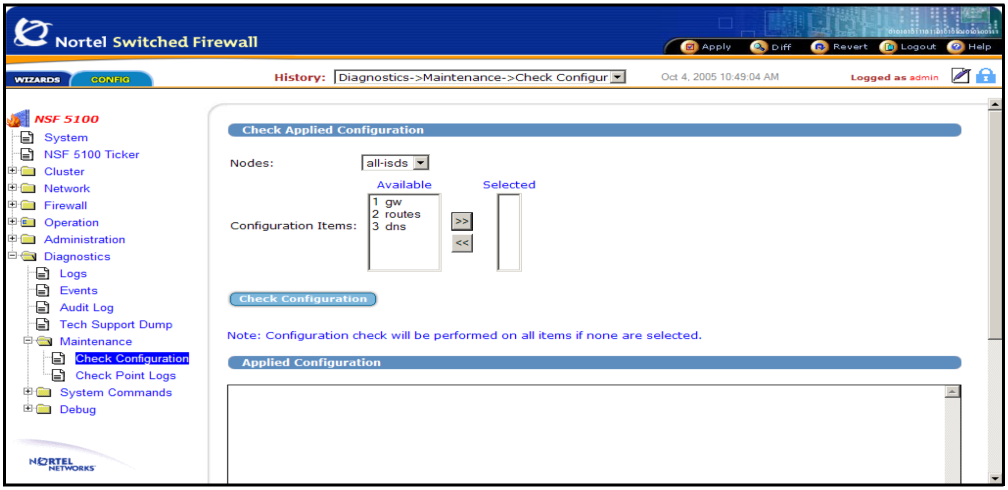
- Firewall Director provides a drop down list containing the IP addresses of the Firewall Directors.
    - Refresh displays the audit information for the selected Firewall Director.
- Time Frame provides two entry fields for setting the time filters for displaying audit information.
    - Begin provides an entry field for setting the begin time filter.
    - End provides an entry field for setting the end time filter.
- Auditing displays the auditing information for the selected Firewall.

Maintenance forms

Use the Diagnostics/Maintenance/Check Configuration form to check the applied configuration (see Diagnostics/Maintenance/Check Configuration form).

Diagnostics/Maintenance/Check Configuration form

Figure 113 Diagnostics/Maintenance/Check Configuration form



History: Diagnostics->Maintenance->Check Configur

Oct 4, 2005 10:49:04 AM

Logged as admin

Check Applied Configuration

Nodes: all-isds

Configuration Items:

Available:
1 gw
2 routes
3 dns

Selected:

Note: Configuration check will be performed on all items if none are selected.

Applied Configuration

The Diagnostics/Maintenance/Check Configuration form is divided into the following two sections:

- Check Applied Configuration
- Applied Configuration

Fields and buttons on the form are as follows:

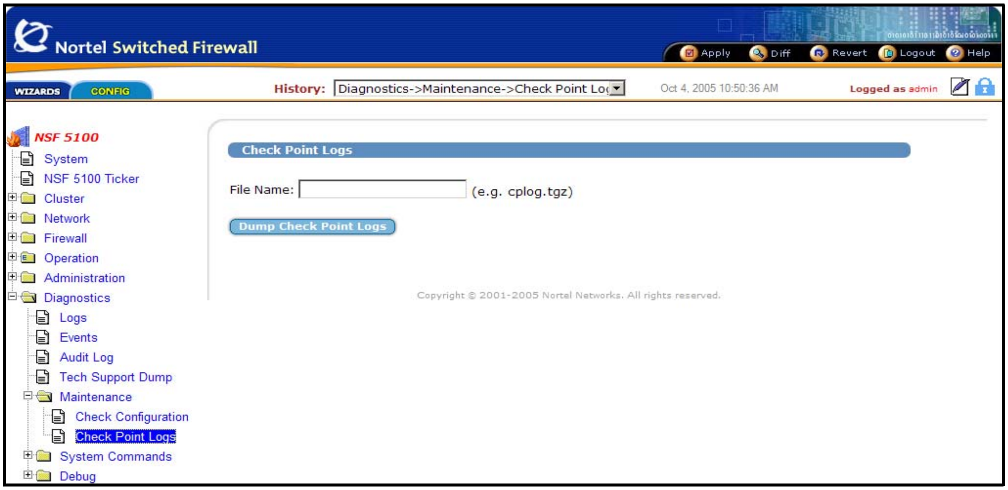
- Check Applied Configuration determines whether the NSF can contact configured gateways, routes, DNS servers, and authentication servers. It also determines whether the NSF can connect to web servers specified in group links.
  - Nodes provides a list with two selections:
    - all-isds performs configuration checks from all hosts.
    - one isd performs configuration checks from local host.
  - Configuration Items provides a list of available configuration items. You can select items from the list or, if selected, remove items from the selected list.
  - Click **Check Configuration** to check the applied configuration. The configuration information appears in the Applied Configuration display area.

- Applied Configuration displays configuration information.

Diagnostics/Maintenance/Check Point Logs form

Use the Diagnostics/Maintenance/Check Point Logs form to provide Check Point Log file information, collected from NSF devices, to the local system for technical support purposes (see Diagnostics/Maintenance/Check Point Logs form).

Figure 114 Diagnostics/Maintenance/Check Point Logs form



History: Diagnostics->Maintenance->Check Point Lo

Oct 4, 2005 10:50:36 AM

Logged as admin

File Name: (e.g. cplog.tgz)

Copyright © 2001-2005 Nortel Networks. All rights reserved.

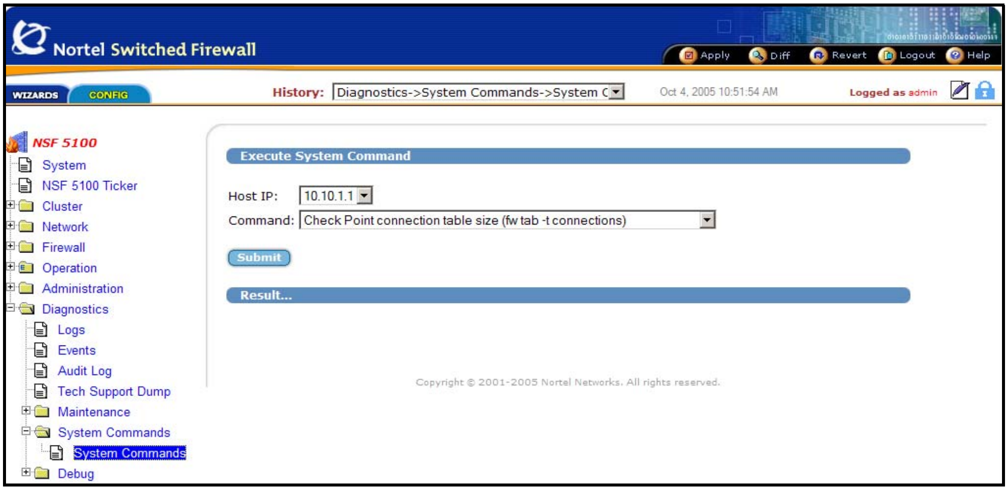
Fields and buttons on the Diagnostics/Maintenance/Check Point Logs form are as follows:

- File Name provides an entry field for the file name used to store the uploaded information.
- To dump the Check Point logs to the specified location, click **Dump Check Point Logs** .

System Commands form

Use the Diagnostics/System Commands/System Commands form to execute Check Point system commands normally entered in a command window (see Diagnostics/System Commands/System Commands form).

Figure 115 Diagnostics/System Commands/System Commands form



History: Diagnostics->System Commands->System C

Oct 4, 2005 10:51:54 AM

Logged as admin

Execute System Command

Host IP: 10.10.1.1

Command: Check Point connection table size (fw tab -t connections)

Result...

Fields and buttons on the Diagnostics/System Commands/System Commands form are as follows:

- Host IP provides a list of host IP addresses.
- Command provides a list of the following Check Point commands:
  - □ Check Point connection table size (fw tab -t connection)
  - □ Check Point connection table size summary (fw tab -t connections -s)
  - □ Check Point interface list (fw ctl iflist)
  - □ Check Point licenses (cplic print -x-t)
  - □ Check Point memory statistics (fw ctl ptstat)
  - □ Check Point policies (fw stat)
  - □ Check Point version (fw ver)
  - □ Check Point Status (fw stat -l)
  - □ Test Sync Network (cphaprob stat)
  - □ Load Check Point Policy (fw fetch localhost)

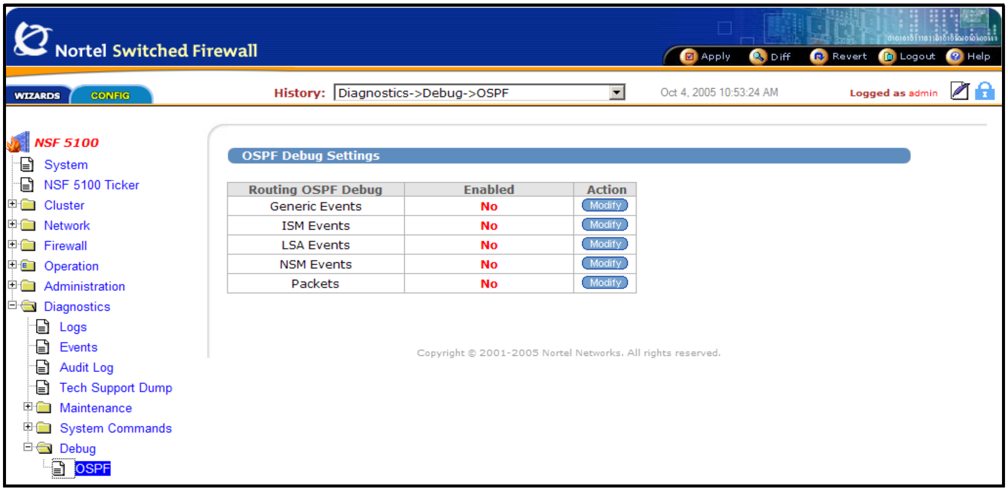
  - □ Unload Check Point Policy (fw unloadlocal)
  - □ Current interfaces (ifconfig)
  - □ Current running processes (ps -aefH)
  - □ Iptables information (iptables -L)
  - □ ARP Table Entries/info/net/arp (arp -n)
- Click **Submit** to execute the selected Check Point command.
- Result displays the result of the selected command execution.

Debug forms

Diagnostics/Debug/OSPF form

Use the Diagnostics/Debug/OSPF form to configure OSPF debug settings (see Diagnostics/Debug/OSPF form).

Figure 116 Diagnostics/Debug/OSPF form



History: Diagnostics->Debug->OSPF

Oct 4, 2005 10:53:24 AM

Logged as admin

OSPF Debug Settings

Routing OSPF Debug	Enabled	Action
Generic Events	No	Modify
ISM Events	No	Modify
LSA Events	No	Modify
NSM Events	No	Modify
Packets	No	Modify

Copyright © 2001-2005 Nortel Networks. All rights reserved.

Fields and buttons on the Diagnostics/Debug/OSPF form are as follows:

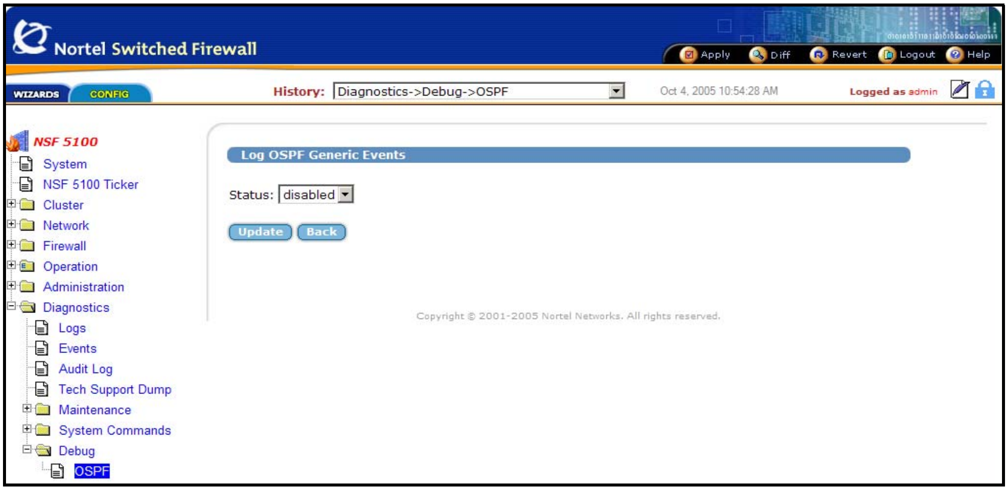
- Routing OSPF Debug displays the following OSPF debugging options:
  - □ Generic Events turns on debugging for OSPF events.
  - □ ISM Events turns on debugging for the interface state machine.
  - □ LSA Events turns on debugging for link state advertisements.
  - □ NSM Events turns on debugging for the neighbor state machine.

  - Packets turns on debugging for OSPF packets.
- Enabled displays the following OSPF Debug operational settings:
  - Yes indicates OSPF Debug is enabled.
  - No indicates OSPF Debug is disabled.
- Action displays a form used to modify a displayed OSPF Debug option.
  - Modify displays a form to modify an OSPF debug option (see Diagnostics/Debug/OSPF Modify form).

Diagnostics/Debug/OSPF Modify form

Use the Diagnostics/Debug/OSPF Modify form to enable or disable logging of OSPF generic events.

Figure 117 Diagnostics/Debug/OSPF Modify form



History: Diagnostics->Debug->OSPF

Log OSPF Generic Events

Status: disabled

Fields and buttons on the Diagnostics/Debug/OSPF Modify form are as follows:

- Status provides a list to select enabled or disabled for logging of OSPF generic events.
- Update submits the change to the pending configuration.
- Back returns to the Diagnostics/Debug/OSPF form without submitting changes to the pending configuration.

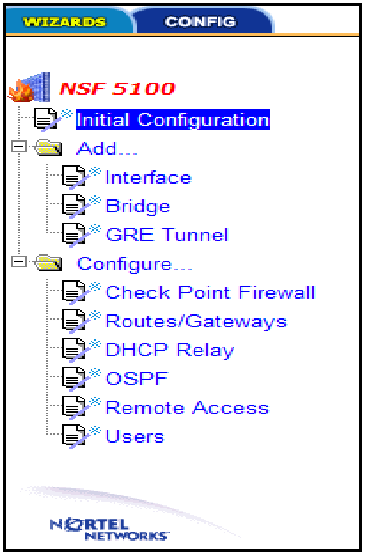
Wizards forms

The Wizards guide the user through configuration processes.

The Wizards tab on the NSF BBI main page provides the following selections (see Wizards main menu):

- Initial Configuration (see Initial Configuration Wizard on page 155)
- Add (see Add Wizard forms on page 156)
    - Interface
    - Bridge
    - GRE Tunnel
- Configure (see Configure Wizard forms on page 157)
    - Check Point Firewall
    - Routes/Gateways
    - DHCP Relay
    - OSPF
    - Remote Access
    - Users

Figure 118 Wizards main menu

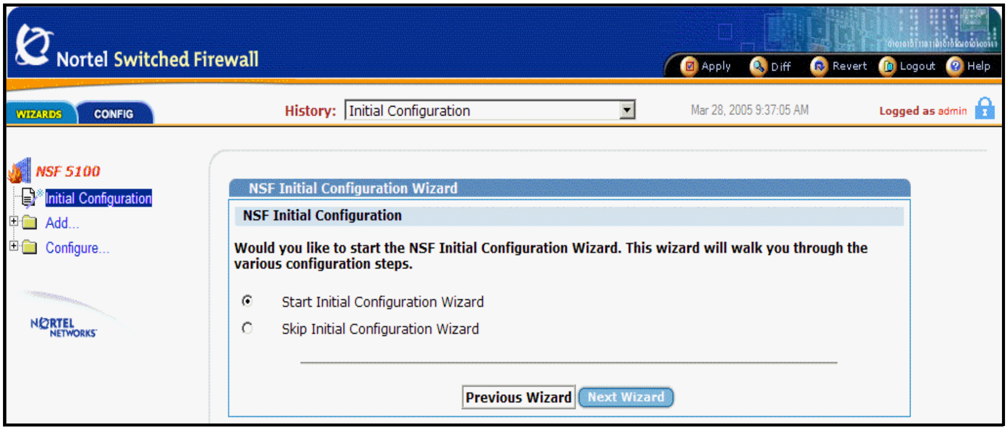


The figures in this section represent the first page of each NSF BBI Wizard.

Initial Configuration Wizard

Use the Initial Configuration wizard to configure a working NSF environment (see Initial Configuration Wizard form).

Figure 119 Initial Configuration Wizard form



History: Initial Configuration

NSF Initial Configuration Wizard

NSF Initial Configuration

Would you like to start the NSF Initial Configuration Wizard. This wizard will walk you through the various configuration steps.

● Start Initial Configuration Wizard

○ Skip Initial Configuration Wizard

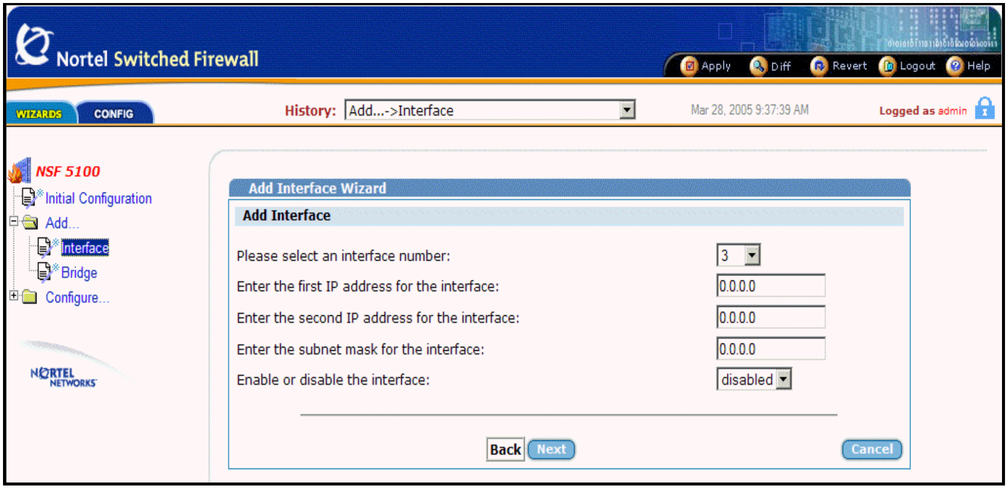
Add Wizard forms

Use the Add forms to add or modify interfaces and bridges.

Add Interface

Use the Add Interface wizard to add a new interface or modify an existing interface (see Add Interface Wizard form).

Figure 120 Add Interface Wizard form



Add Interface Wizard

Add Interface

Please select an interface number: 3

Enter the first IP address for the interface: 0.0.0.0

Enter the second IP address for the interface: 0.0.0.0

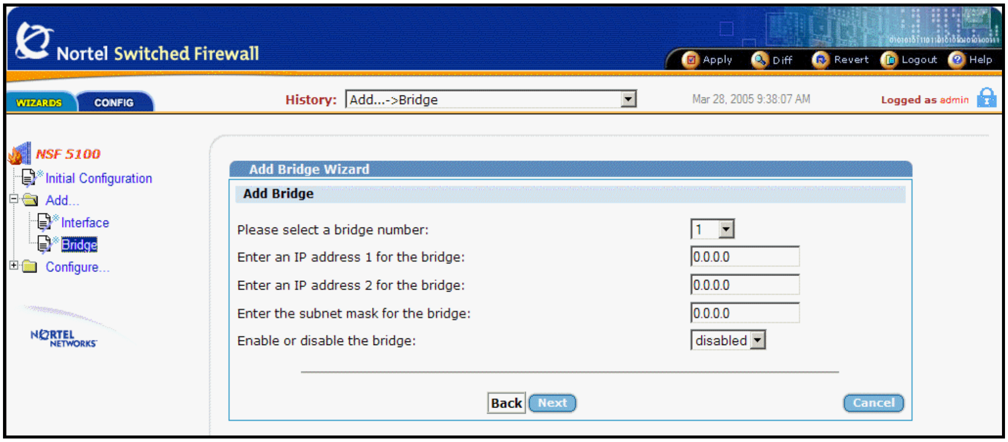
Enter the subnet mask for the interface: 0.0.0.0

Enable or disable the interface: disabled

Add Bridge

Use the Add Bridge wizard to add a bridge to the configuration (see Add Bridge Wizard form).

Figure 121 Add Bridge Wizard form



Add Bridge Wizard

Add Bridge

Please select a bridge number: 1

Enter an IP address 1 for the bridge: 0.0.0.0

Enter an IP address 2 for the bridge: 0.0.0.0

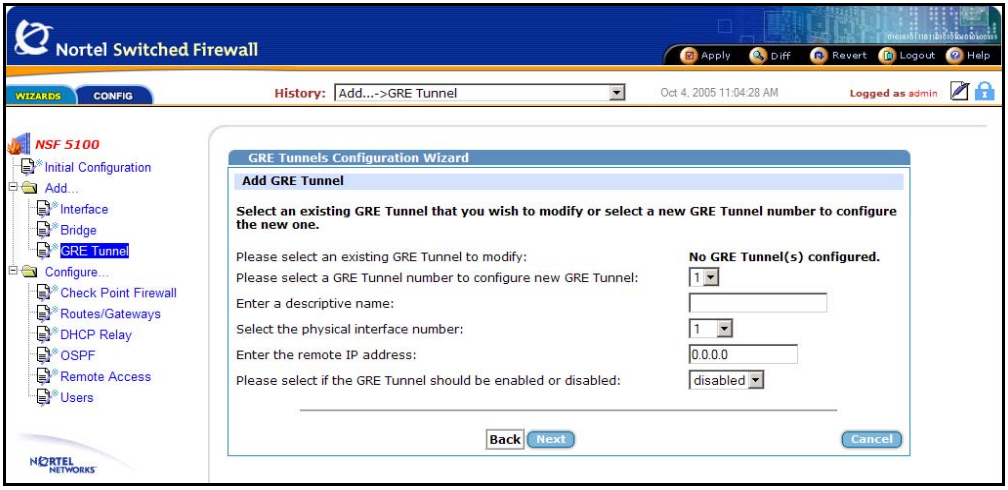
Enter the subnet mask for the bridge: 0.0.0.0

Enable or disable the bridge: disabled

Add GRE Tunnel

Use the Add GRE Tunnel wizard to add a GRE tunnel to the configuration (see Add GRE Tunnel Wizard form).

Figure 122 Add GRE Tunnel Wizard form



History: Add...->GRE Tunnel

GRE Tunnels Configuration Wizard

Add GRE Tunnel

Select an existing GRE Tunnel that you wish to modify or select a new GRE Tunnel number to configure the new one.

Please select an existing GRE Tunnel to modify:	**No GRE Tunnel(s) configured.**
Please select a GRE Tunnel number to configure new GRE Tunnel:	1
Enter a descriptive name:	
Select the physical interface number:	1
Enter the remote IP address:	0.0.0.0
Please select if the GRE Tunnel should be enabled or disabled:	disabled

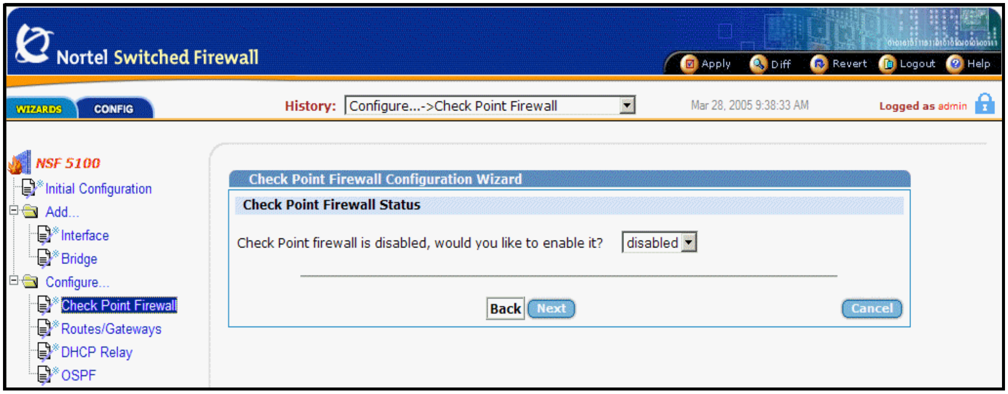
Configure Wizard forms

Use the Configure forms to perform system configurations.

Check Point Firewall

Use the Check Point Firewall form to configure options, such as enabling or disabling Check Point Firewall processing and synchronization status (see Configure Check Point Firewall Wizard form).

Figure 123 Configure Check Point Firewall Wizard form



History: Configure...->Check Point Firewall

Check Point Firewall Configuration Wizard

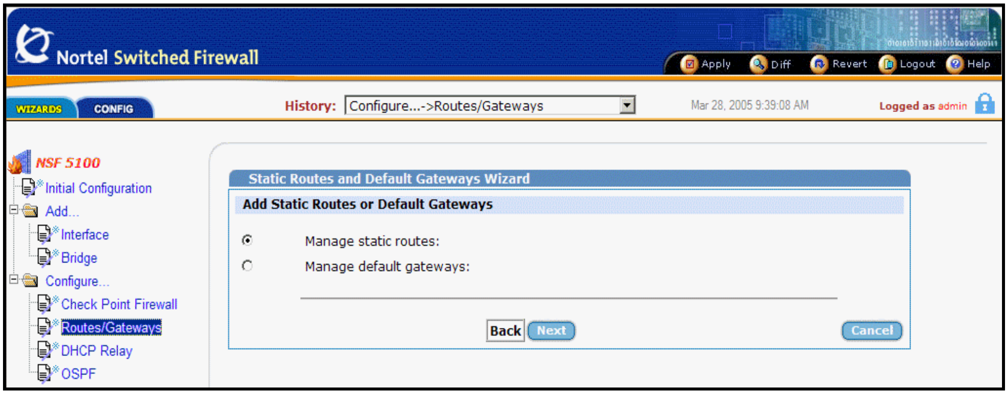
Check Point Firewall Status

Check Point firewall is disabled, would you like to enable it? disabled

Routes/Gateways

Use the Routes/Gateways form to configure static routes and default gateways (Configure Routes/Gateways Wizard form).

Figure 124 Configure Routes/Gateways Wizard form



History: Configure...->Routes/Gateways

Mar 28, 2005 9:39:08 AM

Logged as admin

Static Routes and Default Gateways Wizard

Add Static Routes or Default Gateways

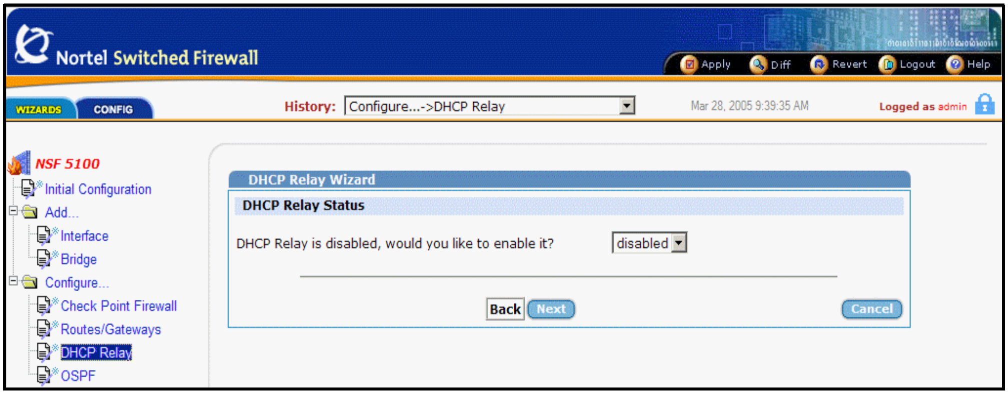
● Manage static routes:

○ Manage default gateways:

DHCP Relay

Use the DHCP Relay form to configure DHCP relay (see Configure DHCP Relay Wizard form).

Figure 125 Configure DHCP Relay Wizard form



History: Configure...->DHCP Relay

Mar 28, 2005 9:39:35 AM

Logged as admin

DHCP Relay Wizard

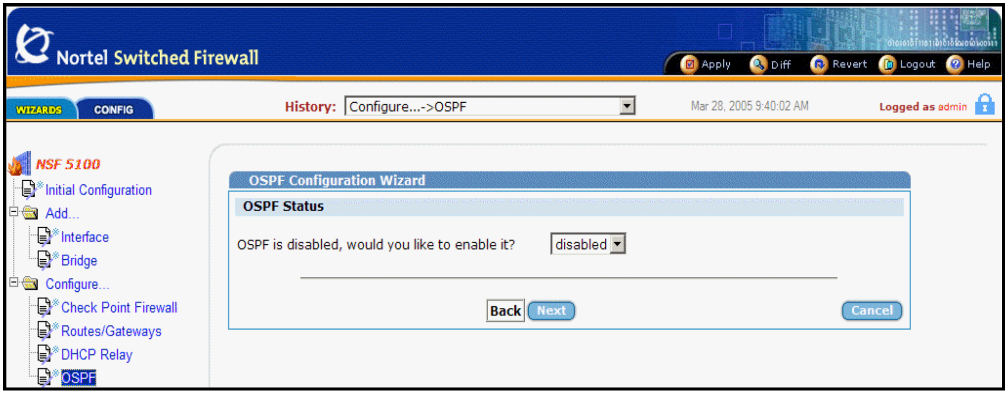
DHCP Relay Status

DHCP Relay is disabled, would you like to enable it? disabled

OSPF

Use the OSPF form to configure use of the Open Shortest Path First (OSPF) protocol (see Configure OSPF Wizard form).

Figure 126 Configure OSPF Wizard form



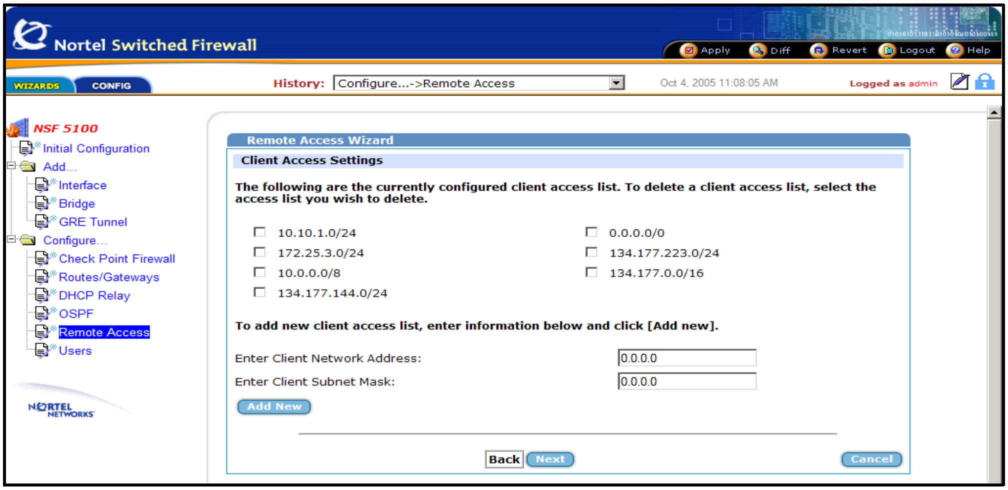
History: Configure...->OSPF

OSPF is disabled, would you like to enable it? disabled

Remote Access

Use the Remote Access wizard form to perform functions associated with remote access configuration, such as add or delete client access lists (see Remote Access Wizard form).

Figure 127 Remote Access Wizard form



History: Configure...->Remote Access

The following are the currently configured client access list. To delete a client access list, select the access list you wish to delete.

□ 10.10.1.0/24	□ 0.0.0.0/0
□ 172.25.3.0/24	□ 134.177.223.0/24
□ 10.0.0.0/8	□ 134.177.0.0/16
□ 134.177.144.0/24	

To add new client access list, enter information below and click [Add new].

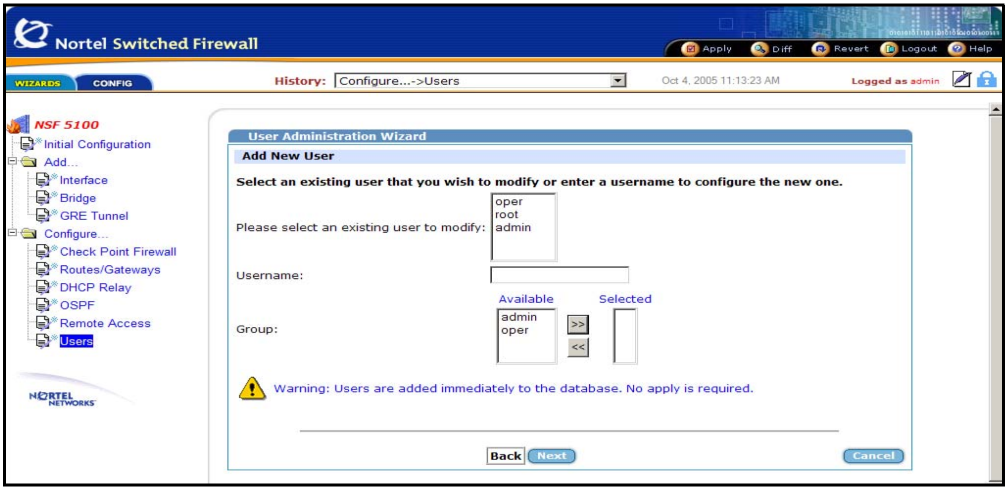
Enter Client Network Address: 0.0.0.0

Enter Client Subnet Mask: 0.0.0.0

Users

Use the User Administration Wizard to perform user administration tasks and configuration, such as add, modify, or delete a user (see User Administration Wizard form).

Figure 128 User Administration Wizard form



History: Configure...->Users

Oct 4, 2005 11:13:23 AM

Logged as admin

User Administration Wizard

Add New User

Select an existing user that you wish to modify or enter a username to configure the new one.

Please select an existing user to modify: oper
root
admin

Username:

Group: Available: admin, oper — Selected:

Warning: Users are added immediately to the database. No apply is required.